Vulnerability Summary for the Week of June 3, 2019

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ais -- logistic_software	SQL Injection in Advanced InfoData Systems (AIS) ESEL-Server 67 (which is the backend for the AIS logistics mobile app) allows an anonymous attacker to execute arbitrary code in the context of the user of the MSSQL database. The default user for the database is the 'sa' user.	2019-05-31	7.5	CVE-2019-10123 MISC MISC
apcupsd -- apcupsd	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an Arbitrary Command Execution issue in apcupsd_status.php.	2019-06-02	7.5	CVE-2019-12585 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- bitbucket	Atlassian Bitbucket Data Center licensed instances starting with version 5.13.0 before 5.13.6 (the fixed version for 5.13.x), from 5.14.0 before 5.14.4 (fixed version for 5.14.x), from 5.15.0 before 5.15.3 (fixed version for 5.15.x), from 5.16.0 before 5.16.3 (fixed version for 5.16.x), from 6.0.0 before 6.0.3 (fixed version for 6.0.x), and from 6.1.0 before 6.1.2 (the fixed version for 6.1.x) allow remote attackers who have admin permissions to achieve remote code execution on a Bitbucket server instance via path traversal through the Data Center migration tool.	2019-06-03	9.0	CVE-2019-3397 MISC
atlassian -- crowd	Atlassian Crowd and Crowd Data Center had the pdkinstall development plugin incorrectly enabled in release builds. Attackers who can send unauthenticated or authenticated requests to a Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permits remote code execution on systems running a vulnerable version of Crowd or Crowd Data Center. All versions of Crowd from version 2.1.0 before 3.0.5 (the fixed version for 3.0.x), from version 3.1.0 before 3.1.6 (the fixed version for 3.1.x), from version 3.2.0 before 3.2.8 (the fixed version for 3.2.x), from version 3.3.0 before 3.3.5 (the fixed version for 3.3.x), and from version 3.4.0 before 3.4.4 (the fixed	2019-06-03	7.5	CVE-2019-11580 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	version for 3.4.x) are affected by this vulnerability.			
aubio -- aubio	aubio v0.4.0 to v0.4.8 has a Buffer Overflow (issue 1 of 3).	2019-06-07	7.5	CVE-2018-19800 MISC
cyrus -- imap	The CalDAV feature in httpd in Cyrus IMAP 2.5.x through 2.5.12 and 3.0.x through 3.0.9 allows remote attackers to execute arbitrary code via a crafted HTTP PUT operation for an event with a long iCalendar property name.	2019-06-03	7.5	CVE-2019-11356 FEDORA FEDORA BUGTRAQ MISC MISC MISC MISC DEBIAN
exim -- exim	A flaw was found in Exim versions 4.87 to 4.91 (inclusive). Improper validation of recipient address in deliver_message() function in /src/deliver.c may lead to remote command execution.	2019-06-05	7.5	CVE-2019-10149 SUSE MISC MLIST MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MLIST BID CONFIRM BUGTRAQ GENTOO UBUNTU DEBIAN CONFIRM
facebook -- osquery	In some configurations an attacker can inject a new executable path into the extensions.load file for osquery and hard link a parent folder of a malicious binary to a folder with known 'safe' permissions. Under those circumstances osquery will load said malicious executable with SYSTEM permissions. The solution is to migrate installations to the 'Program Files' directory on Windows which restricts unprivileged write access. This issue affects osquery prior to v3.4.0.	2019-06-03	9.3	CVE-2019-3567 MISC
ffmpeg -- ffmpeg	aa_read_header in libavformat/aadec.c in FFmpeg before 3.2.14 does not check for sscanf failure and consequently allows use of uninitialized variables.	2019-06-04	7.5	CVE-2019-12730 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi_dashboard_project -- glpi_dashboard	Incorrect access control was discovered in the stdonato Dashboard plugin through 0.9.7 for GLPI, affecting df.php, issue.php, load.php, mem.php, traf.php, and uptime.php in front/sh.	2019-06-02	7.5	CVE-2019-12530 MISC
godotengine -- godot	In Godot through 3.1, remote code execution is possible due to the deserialization policy not being applied correctly.	2019-05-31	7.5	CVE-2019-10069 MISC MISC
hoteldruid -- hoteldruid	HotelDruid before v2.3.1 has SQL Injection via the /visualizza_tabelle.php anno parameter.	2019-06-07	7.5	CVE-2019-9086 MISC MISC
hoteldruid -- hoteldruid	HotelDruid before v2.3.1 has SQL Injection via the /tab_tariffe.php numtariffa1 parameter.	2019-06-07	7.5	CVE-2019-9087 MISC MISC
hp -- integrated_lights-out_4_firmware	A remote cross site scripting vulnerability was identified in HPE Integrated Lights-Out 4 (iLO 4) earlier than v2.61b for Gen9 servers and Integrated Lights-Out 5 (iLO 5) for Gen10 Servers earlier than version v1.39.	2019-06-05	7.6	CVE-2019-11982 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- integrated_lights-out_4_firmware	A remote buffer overflow vulnerability was identified in HPE Integrated Lights-Out 4 (iLO 4) earlier than v2.61b for Gen9 servers and Integrated Lights-Out 5 (iLO 5) for Gen10 Servers earlier than version v1.39.	2019-06-05	8.3	CVE-2019-11983 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2018-7121 CONFIRM
hp -- intelligent_management_center	A remote denial of service vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	7.8	CVE-2018-7123 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2018-7124 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11941 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent	2019-06-05	9.0	CVE-2019-11942

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Management Center (IMC) PLAT earlier than version 7.3 E0506P09.			CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11943 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-11944 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-11945 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11947 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11948 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-11949 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11950 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11951 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11952 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11953 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11954 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11955 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11956 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.3	CVE-2019-11957 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11958 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11959 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11960 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11961 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11962 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11963 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11964 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11965 CONFIRM
hp -- intelligent_management_center	A remote privilege escalation vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11966 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11967 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11968 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11969 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11970 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11971 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11972 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11973 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11974 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11975 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11976 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11977 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11978 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11979 CONFIRM
hp -- intelligent_management_center	A remote code exection vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11980 CONFIRM
hp -- intelligent_management_center	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11984 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11985 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-11986 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5338 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5339 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5340 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5341 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5342 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5343 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5344 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5345 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5346 CONFIRM
hp -- intelligent_management_center	A remote authentication bypass vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5347 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5348 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5349 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5350 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5351 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5352 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5353 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5354 CONFIRM
hp -- intelligent_management_center	A remote denial of service vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	7.8	CVE-2019-5355 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5356 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5357 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5358 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5359 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5360 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5361 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5362 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5363 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5364 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5365 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5366 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5367 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5368 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5369 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5370 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5371 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5372 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5373 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5374 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5375 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5376 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5377 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5378 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5379 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5380 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5381 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5382 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5383 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5384 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5385 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5386 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5387 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5388 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	9.0	CVE-2019-5389 CONFIRM
hp -- intelligent_management_center	A remote command injection vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5390 CONFIRM
hp -- intelligent_management_center	A stack buffer overflow vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	10.0	CVE-2019-5391 CONFIRM
huawei -- s12700_firmware	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to	2019-06-04	7.8	CVE-2019-5285 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109)			
ivanti -- landesk_management_suite	Open directories in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 may lead to remote information disclosure and arbitrary code execution.	2019-06-03	7.5	CVE-2019-12375 MISC
ivanti -- landesk_management_suite	A vulnerable upl/async_upload.asp web API endpoint in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 allows arbitrary file upload, which may lead to arbitrary remote code execution.	2019-06-03	7.5	CVE-2019-12377 MISC MISC
jector -- fm-k75_firmware	Jector Smart TV FM-K75 devices allow remote code execution because there is an adb open port with root permission.	2019-05-31	10.0	CVE-2019-9871 MISC MISC
kromtech -- mackeeper	Kromtech MacKeeper 3.20.4 suffers from a root privilege escalation vulnerability through its `com.mackeeper.AdwareAnalyzer.AdwareAnalyzerPrivilegedHelper` component. The AdwareAnalzyerPrivilegedHelper tool implements an XPC service that	2019-06-05	10.0	CVE-2018-10171 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows an unprivileged application to connect and execute shell scripts as the root user.			
linksys -- wrt1900acs_firmware	An issue was discovered on Linksys WRT1900ACS 1.0.3.187766 devices. A lack of encryption in how the user login cookie (admin-auth) is stored on a victim's computer results in the admin password being discoverable by a local attacker, and usable to gain administrative access to the victim's router. The admin password is stored in base64 cleartext in an "admin-auth" cookie. An attacker sniffing the network at the time of login could acquire the router's admin password. Alternatively, gaining physical access to the victim's computer soon after an administrative login could result in compromise.	2019-06-06	7.2	CVE-2019-7311 MISC MISC
linux -- linux_kernel	An issue was discovered in dlpar_parse_cc_property in arch/powerpc/platforms/pseries/dlpar.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup of prop->name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	2019-06-03	7.8	CVE-2019-12614 BID MISC MISC
linux -- linux_kernel	An issue was discovered in get_vdev_port_node_info in arch/sparc/kernel/mdesc.c in the Linux kernel through 5.1.6. There is an	2019-06-03	7.8	CVE-2019-12615 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unchecked kstrdup_const of node_info->vdev_port.name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).			MISC MISC
linux -- linux_kernel	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network.	2019-06-03	8.3	CVE-2019-3846 CONFIRM FEDORA FEDORA MISC
microfocus -- service_manager	Remote unauthorized command execution and unauthorized disclosure of information in Micro Focus Service Manager, versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61. This vulnerability could allow Remote unauthorized command execution and unauthorized disclosure of information.	2019-06-03	9.0	CVE-2019-11646 MISC
northern -- cfengine	Northern.tech CFEngine Enterprise 3.12.1 has Insecure Permissions.	2019-06-06	9.0	CVE-2019-9929 MISC MISC
orpak -- siteomat	The Orpak SiteOmat OrCU component is vulnerable to code	2019-06-03	10.0	CVE-2017-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection, for all versions prior to 2017-09-25, due to a search query that uses a direct shell command. By tampering with the request, an attacker is able to run shell commands and receive valid output from the device.			14853 BID MISC MISC
orpak -- siteomat	A stack buffer overflow exists in one of the Orpak SiteOmat CGI components, allowing for remote code execution. The vulnerability affects all versions prior to 2017-09-25.	2019-06-03	7.5	CVE-2017-14854 MISC BID MISC
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin before 4.9.0.1. A vulnerability was reported where a specially crafted database name can be used to trigger an SQL injection attack through the designer feature.	2019-06-05	7.5	CVE-2019-11768 BID CONFIRM
primasystems -- flexair	Prima Systems FlexAir devices have Hard-coded Credentials.	2019-06-05	7.5	CVE-2019-7672 MISC MISC MISC
primasystems -- flexair	On Prima Systems FlexAir devices through 2.4.9api3, an authenticated user can upload Python (.py) scripts and execute arbitrary code with root privileges.	2019-06-05	9.0	CVE-2019-9189 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pydio -- pydio	The ImageMagick plugin that is installed by default in Pydio through 8.2.2 does not perform the appropriate validation and sanitization of user supplied input in the plugin's configuration options, allowing arbitrary shell commands to be entered that result in command execution on the underlying operating system, with the privileges of the local user running the web server. The attacker must be authenticated into the application with an administrator user account in order to be able to edit the affected plugin configuration.	2019-05-31	9.0	CVE-2019-10048 MISC
pydio -- pydio	An issue was discovered in proxy.php in pydio-core in Pydio through 8.2.2. Through an unauthenticated request, it possible to evaluate malicious PHP code by placing it on the fourth line of a .php file, as demonstrated by a PoC.php created by the guest account, with execution via a proxy.php?hash=../../../../../var/lib/pydio/data/personal/guest/PoC.php request. This is related to plugins/action.share/src/Store/ShareStore.php.	2019-06-05	7.5	CVE-2019-9642 MISC CONFIRM
qemu -- qemu	In QEMU 3.1.0, load_device_tree in device_tree.c calls the deprecated load_image function, which has a buffer overflow risk.	2019-05-31	7.5	CVE-2018-20815 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rakuten -- viber	A vulnerability in Viber before 10.7.0 for Desktop (Windows) could allow an attacker to execute arbitrary commands on a targeted system. This vulnerability is due to unsafe search paths used by the application URI. An attacker could exploit this vulnerability by convincing a targeted user to follow a malicious link. Successful exploitation could cause the application to load libraries from the directory targeted by the URI link. The attacker could use this behavior to execute arbitrary commands on the system with the privileges of the targeted user, if the attacker can place a crafted library in a directory that is accessible to the vulnerable system.	2019-06-02	9.3	CVE-2019-12569 MISC
rubygems -- rubygems	A Directory Traversal issue was discovered in RubyGems 2.7.6 and later through 3.0.2. Before making new directories or touching files (which now include path-checking code for symlinks), it would delete the target destination. If that destination was hidden behind a symlink, a malicious gem could delete arbitrary files on the user's machine, presuming the attacker could guess at paths. Given how frequently gem is run as sudo, and how predictable paths are on modern systems (/tmp, /usr, etc.), this could likely lead to data loss or an unusable system.	2019-06-06	8.8	CVE-2019-8320 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
saet -- webapp	The WebApp v04.68 in the supervisor on SAET Impianti Speciali TEBE Small 05.01 build 1137 devices allows remote attackers to execute or include local .php files, as demonstrated by menu=php://filter/convert.base64-encode/resource=index.php to read index.php.	2019-05-31	7.5	CVE-2019-9106 MISC MISC
sitecore -- cms	Deserialization of Untrusted Data in the Sitecore.Security.AntiCSRF (aka anti CSRF) module in Sitecore CMS 7.0 to 7.2 and Sitecore XP 7.5 to 8.2 allows an unauthenticated attacker to execute arbitrary code by sending a serialized .NET object in the HTTP POST parameter __CSRFTOKEN.	2019-05-31	7.5	CVE-2019-9874 MISC MISC MISC
sweetscape -- 010_editor	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the StrCat function (provided by the scripting engine) allows an attacker to overwrite arbitrary memory, which could lead to code execution.	2019-06-05	7.5	CVE-2019-12553 MISC CONFIRM
titanhq -- spamtitan	In TitanHQ SpamTitan through 7.03, a vulnerability exists in the spam rule update function. Updates are downloaded over HTTP, including scripts which are subsequently executed with root permissions. An attacker with a privileged network position is trivially able to inject arbitrary commands.	2019-06-05	8.5	CVE-2019-6800 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tldp -- advanced_bash-scripting_guide	The function getopt_simple as described in Advanced Bash Scripting Guide (ISBN 978-1435752184) allows privilege escalation and execution of commands when used in a shell script called, for example, via sudo.	2019-05-31	10.0	CVE-2019-9891 MISC
ui -- aircam_firmware	On Ubiquiti airCam 3.1.4 devices, a Denial of Service vulnerability exists in the RTSP Service provided by the ubnt-streamer binary. The issue can be triggered via malformed RTSP requests that lead to an invalid memory read. To exploit the vulnerability, an attacker must craft an RTSP request with a large number of headers.	2019-06-04	7.8	CVE-2019-12727 MISC
vim -- vim	getchar.c in Vim before 8.1.1365 and Neovim before 0.3.6 allows remote attackers to execute arbitrary OS commands via the :source! command in a modeline, as demonstrated by execute in Vim, and assert_fails or nvim_input in Neovim.	2019-06-05	9.3	CVE-2019-12735 MISC MISC MISC MISC MISC FEDORA
zohocorp -- manageengine_netflow_analyzer	A SQL injection vulnerability in /client/api/json/v2/nfareports/compareReport in Zoho ManageEngine NetFlow Analyzer 12.3 allows attackers to execute arbitrary SQL commands via the DeviceID parameter.	2019-06-05	7.5	CVE-2019-12196 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zyxel -- p-660hn-t1_firmware	The rpWLANRedirect.asp ASP page is accessible without authentication on ZyXEL P-660HN-T1 V2 (2.00(AAKK.3)) devices. After accessing the page, the admin user's password can be obtained by viewing the HTML source code, and the interface of the modem can be accessed as admin.	2019-05-31	10.0	CVE-2019-6725 BUGTRAQ

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apcupsd -- apcupsd	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an XSS issue in apcupsd_status.php.	2019-06-02	4.3	CVE-2019-12584 MISC MISC MISC
atutor -- atutor	ATutor 2.2.4 allows Arbitrary File Upload and Directory Traversal, resulting in remote code execution	2019-06-03	6.8	CVE-2019-1216

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via a ".." pathname in a ZIP archive to the mods/_core/languages/language_import.php (aka Import New Language) or mods/_standard/patcher/index_admin.php (aka Patcher) component.			9 MISC MISC MISC
aubio -- aubio	aubio v0.4.0 to v0.4.8 has a NULL pointer dereference (issue 1 of 6).	2019-06-07	5.0	CVE-2018-19801 MISC
aubio -- aubio	aubio v0.4.0 to v0.4.8 has a Buffer Overflow (issue 2 of 3).	2019-06-07	5.0	CVE-2018-19802 MISC
bitdefender -- safepay	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Bitdefender SafePay 23.0.10.34. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of tiscript. When processing the System.Exec method the application does not properly validate a user-supplied string before using it to	2019-06-03	6.8	CVE-2019-6736 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execute a system call. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7234.			
bitdefender -- safepay	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Bitdefender SafePay 23.0.10.34. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIScript. The issue lies in the handling of the openFile method, which allows for an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability execute code in the context of the current process. Was ZDI-CAN-7247.	2019-06-03	6.8	CVE-2019-6737 CONFIRM MISC
bitdefender -- safepay	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Bitdefender SafePay 23.0.10.34. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIScript. When processing the launch method the application does not properly validate a user-supplied	2019-06-03	6.8	CVE-2019-6738 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	string before using it to execute a system call. An attacker can leverage this vulnerability execute code in the context of the current process. Was ZDI-CAN-7250.			
bludit -- bludit	Bludit before 3.9.0 allows remote code execution for an authenticated user by uploading a php file while changing the logo through /admin/ajax/upload-logo.	2019-06-03	6.5	CVE-2019-12548 CONFIRM MISC CONFIRM
bludit -- bludit	Bludit prior to 3.9.1 allows a non-privileged user to change the password of any account, including admin. This occurs because of bl-kernel/admin/controllers/user-password.php Insecure Direct Object Reference (a modified username POST parameter).	2019-06-05	6.5	CVE-2019-12742 MISC MISC
cisco -- enterprise_chat_and_email	A vulnerability in the web-based management interface of Cisco Enterprise Chat and Email (ECE) Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-	2019-06-05	4.3	CVE-2019-1870 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web interface or allow the attacker to access sensitive browser-based information.			
cisco -- industrial_network_director	A vulnerability in the web-based management interface of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on an affected device. For more information about CSRF attacks and potential mitigations, see	2019-06-05	6.8	CVE-2019-1881 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Understanding Cross-Site Request Forgery Threat Vectors.			
cisco -- ios_xr_firmware	A vulnerability in the Secure Shell (SSH) authentication function of Cisco IOS XR Software could allow an authenticated, remote attacker to successfully log in to an affected device using two distinct usernames. The vulnerability is due to a logic error that may occur when certain sequences of actions are processed during an SSH login event on the affected device. An attacker could exploit this vulnerability by initiating an SSH session to the device with a specific sequence that presents the two usernames. A successful exploit could result in logging data misrepresentation, user enumeration, or, in certain circumstances, a command authorization bypass. See the Details section for more information.	2019-06-05	5.5	CVE-2019-1842 BID CISCO
cisco -- telepresence_video_communication_server	A vulnerability in the authentication service of the Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, Cisco TelePresence Video Communication Server (VCS), and Cisco Expressway Series could allow an unauthenticated, remote attacker to cause a service outage for users attempting to authenticate, resulting in a denial of service (DoS)	2019-06-05	5.0	CVE-2019-1845 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	condition. The vulnerability is due to insufficient controls for specific memory operations. An attacker could exploit this vulnerability by sending a malformed Extensible Messaging and Presence Protocol (XMPP) authentication request to an affected system. A successful exploit could allow the attacker to cause an unexpected restart of the authentication service, preventing users from successfully authenticating. Exploitation of this vulnerability does not impact users who were authenticated prior to an attack.			
cisco -- telepresence_video_communication_server	A vulnerability in Cisco TelePresence Video Communication Server (VCS) and Cisco Expressway Series software could allow an unauthenticated, remote attacker to cause an affected system to send arbitrary network requests. The vulnerability is due to improper restrictions on network services in the affected software. An attacker could exploit this vulnerability by sending malicious requests to the affected system. A successful exploit could allow the attacker to send arbitrary network requests sourced from the affected system.	2019-06-05	5.0	CVE-2019-1872 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- webex_meetings_server	A vulnerability in the web-based management interface of Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to access sensitive system information. The vulnerability is due to improper access control to files within the web-based management interface. An attacker could exploit this vulnerability by sending a malicious request to an affected device. A successful exploit could allow the attacker to access sensitive system information.	2019-06-05	5.0	CVE-2019-1868 BID CISCO
citrix -- xenmobile_server	An Incorrect Access Control vulnerability has been identified in Citrix XenMobile Server 10.8.0 before Rolling Patch 6 and 10.9.0 before Rolling Patch 3. An attacker can impersonate and take actions on behalf of any Mobile Application Management (MAM) enrolled device.	2019-06-05	6.4	CVE-2018-18571 BID CONFIRM
cloudera -- cloudera_manager	This CVE relates to an unspecified cross site scripting vulnerability in Cloudera Manager.	2019-06-07	4.3	CVE-2018-5798 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dameware -- remote_mini_control	Dameware Remote Mini Control version 12.1.0.34 and prior contains an unauthenticated remote buffer over-read due to the server not properly validating CltDHPubKeyLen during key negotiation, which could crash the application or leak sensitive information.	2019-06-07	5.8	CVE-2019-3956 MISC
dameware -- remote_mini_control	Dameware Remote Mini Control version 12.1.0.34 and prior contains an unauthenticated remote buffer over-read due to the server not properly validating RsaSignatureLen during key negotiation, which could crash the application or leak sensitive information.	2019-06-07	5.8	CVE-2019-3957 MISC
djangoproject -- django	An issue was discovered in Django 1.11 before 1.11.21, 2.1 before 2.1.9, and 2.2 before 2.2.2. The clickable Current URL value displayed by the AdminURLFieldWidget displays the provided value without validating it as a safe URL. Thus, an unvalidated value stored in the database, or a value provided as a URL query parameter payload, could result in an clickable JavaScript link.	2019-06-03	4.3	CVE-2019-12308 MLIST BID CONFIRM CONFIRM CONFIRM MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CMIS CMLIST CONFIRM
douco -- douphp	In DouCo DouPHP v1.5 Release 20190516, remote attackers can view the database backup file via a brute-force guessing approach for data/backup/DyyyymmddThhmmss.sql filenames.	2019-06-02	5.0	CVE-2019-12564 MISC
eficode -- influxdb	Jenkins InfluxDB Plugin 1.21 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2019-05-31	4.0	CVE-2019-10329 MLIST BID MISC
evernote -- evernote	Evernote 7.9 on macOS allows attackers to execute arbitrary programs by embedding a reference to a local executable file such as the /Applications/Calculator.app/Contents/MacOS/Calculator file.	2019-05-31	4.4	CVE-2019-10038 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
exagrid -- backup_appliance_firmware	ExaGrid appliances with firmware version v4.8.1.1044.P50 have a /monitor/data/Upgrade/ directory traversal vulnerability, which allows remote attackers to view and retrieve verbose logging information. Files within this directory were observed to contain sensitive run-time information, including Base64 encoded 'support' credentials, leading to administrative access of the device.	2019-06-03	5.0	CVE-2019-12310 MISC MISC
firejail_project -- firejail	In Firejail before 0.9.60, seccomp filters are writable inside the jail, leading to a lack of intended seccomp restrictions for a process that is joined to the jail after a filter has been modified by an attacker.	2019-06-02	4.6	CVE-2019-12589 MISC MISC MISC
fortinet -- fortios	An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.	2019-06-04	5.0	CVE-2018-13379 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortios	A Cross-site Scripting (XSS) vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.7, 5.4 and below versions under SSL VPN web portal allows attacker to execute unauthorized malicious script code via the error or message handling parameters.	2019-06-04	4.3	CVE-2018-13380 BID CONFIRM
fortinet -- fortios	A buffer overflow vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.7, 5.4 and below versions under SSL VPN web portal allows a non-authenticated attacker to perform a Denial-of-service attack via special craft message payloads.	2019-06-04	5.0	CVE-2018-13381 BID CONFIRM
fortinet -- fortios	An Improper Authorization vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.8 and 5.4.1 to 5.4.10 under SSL VPN web portal allows an unauthenticated attacker to modify the password of an SSL VPN web portal user via specially crafted HTTP requests.	2019-06-04	5.0	CVE-2018-13382 CONFIRM
fortinet -- fortios	A Host Header Redirection vulnerability in Fortinet FortiOS all versions below 6.0.5 under SSL VPN web portal allows a remote attacker to potentially poison HTTP cache and subsequently redirect SSL VPN web portal users to arbitrary web domains.	2019-06-04	5.8	CVE-2018-13384 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortios	A reflected Cross-Site-Scripting (XSS) vulnerability in Fortinet FortiOS 5.2.0 to 6.0.4 under SSL VPN web portal may allow an attacker to execute unauthorized malicious script code via the "param" parameter of the error process HTTP requests.	2019-06-04	4.3	CVE-2019-5586 BID CONFIRM
fortinet -- fortios	Lack of root file system integrity checking in Fortinet FortiOS VM application images all versions below 6.0.5 may allow attacker to implant malicious programs into the installing image by reassembling the image through specific methods.	2019-06-04	4.0	CVE-2019-5587 BID CONFIRM
fortinet -- fortios	A reflected Cross-Site-Scripting (XSS) vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4 under SSL VPN web portal may allow an attacker to execute unauthorized malicious script code via the "err" parameter of the error process HTTP requests.	2019-06-04	4.3	CVE-2019-5588 BID CONFIRM
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit PhantomPDF 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within	2019-06-03	4.3	CVE-2019-6752 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the parsing of PDF documents. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7620.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.3.0.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Stuff method. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before writing to memory. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7561.	2019-06-03	4.3	CVE-2019-6753 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this	2019-06-03	6.8	CVE-2019-6754 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the localFileStorage method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7407.			MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7613.	2019-06-03	6.8	CVE-2019-6755 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit PhantomPDF 9.4.0.16811. User interaction is	2019-06-03	4.3	CVE-2019-6756 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of HTML files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7769.			MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7696.	2019-06-03	6.8	CVE-2019-6757 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader	2019-06-03	4.3	CVE-2019-6758 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7701.			CMISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7614.	2019-06-03	6.8	CVE-2019-6759 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7694.	2019-06-03	6.8	CVE-2019-6760 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.0.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the XFA CXFA_FFDocView object. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7777.	2019-06-03	6.8	CVE-2019-6761 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit PhantomPDF 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7844.	2019-06-03	6.8	CVE-2019-6762 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the ToggleFormsDesign method of the Foxit.FoxitReader.Ctl ActiveX object. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the	2019-06-03	6.8	CVE-2019-6763 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	current process. Was ZDI-CAN-7874.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA Template objects. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7972.	2019-06-03	6.8	CVE-2019-6764 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit PhantomPDF 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this	2019-06-03	6.8	CVE-2019-6765 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to execute code in the context of the current process. Was ZDI-CAN-8170.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8162.	2019-06-03	4.3	CVE-2019-6766 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence	2019-06-03	6.8	CVE-2019-6767 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8163.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8164.	2019-06-03	6.8	CVE-2019-6768 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing	2019-06-03	6.8	CVE-2019-6769 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8165.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the resetForm method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8229.	2019-06-03	4.3	CVE-2019-6770 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 2019.010.20098. User interaction is required to exploit this vulnerability in that the target must visit a	2019-06-03	4.3	CVE-2019-6771 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious page or open a malicious file. The specific flaw exists within the handling of the value property of a Field object within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8230.			
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 2019.010.20098. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8231.	2019-06-03	4.3	CVE-2019-6772 MISC MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to disclose sensitive information on vulnerable	2019-06-03	4.3	CVE-2019-6773

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the richValue property of a Field object within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8272.			MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7634.	2019-06-03	4.3	CVE-2019-6746 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZI files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7636.	2019-06-03	6.8	CVE-2019-6747 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZI files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7637.	2019-06-03	6.8	CVE-2019-6748 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZIX files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7638.	2019-06-03	6.8	CVE-2019-6749 MISC MISC
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZI files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7639.	2019-06-03	6.8	CVE-2019-6750 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_studio_photo	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6.779. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7632.	2019-06-03	6.8	CVE-2019-6751 MISC MISC
gardener -- gardener	In Gardener before 0.20.0, incorrect access control in seed clusters allows information disclosure by sending HTTP GET requests from one's own shoot clusters to foreign shoot clusters. This occurs because traffic from shoot to seed via the VPN endpoint is not blocked.	2019-06-05	5.0	CVE-2019-12494 MISC MISC CONFIRM
gilacms -- gila_cms	Gila CMS 1.9.1 has XSS.	2019-06-05	4.3	CVE-2019-9647 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
gitea -- gitea	Jenkins Gitea Plugin 1.1.1 and earlier did not implement trusted revisions, allowing attackers without commit access to the Git repo to change Jenkinsfiles even if Jenkins is configured to consider them to be untrusted.	2019-05-31	5.0	CVE-2019-10330 MLIST BID MISC
glyphandcog -- xpdfreader	There is an out-of-bounds read vulnerability in the function FlateStream::getChar() located at Stream.cc in Xpdf 4.01.01. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an attacker to cause Information Disclosure or a denial of service.	2019-06-01	5.8	CVE-2019-12515 MISC
grails -- grails	Grails before 3.3.10 used cleartext HTTP to resolve the SDKMan notification service. NOTE: users' apps were not resolving dependencies over cleartext HTTP.	2019-06-04	6.8	CVE-2019-12728 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
grandnode -- grandnode	A Path Traversal vulnerability in Controllers/LetsEncryptController.cs in LetsEncryptController in GrandNode 4.40 allows remote, unauthenticated attackers to retrieve arbitrary files on the web server via specially crafted LetsEncrypt/Index?fileName= HTTP requests. A patch for this issue was made on 2019-05-30 in GrandNode 4.40.	2019-06-05	5.0	CVE-2019-12276 MISC MISC
hp -- intelligent_management_center	A remote disclosure of information vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	5.0	CVE-2018-7122 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	6.5	CVE-2018-7125 CONFIRM
hp -- intelligent_management_center	A remote credential disclosure vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	6.8	CVE-2019-11946 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- intelligent_management_center	A disclosure of information vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	5.0	CVE-2019-5392 CONFIRM
hp -- intelligent_management_center	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	2019-06-05	6.8	CVE-2019-5393 CONFIRM
huawei -- ar1200-s_firmware	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device.	2019-06-04	4.6	CVE-2019-5300 CONFIRM
ibm -- control_desk	IBM Maximo Asset Management 7.6 could allow a an authenticated user to replace a target page with a phishing site which could allow the attacker to obtain highly sensitive	2019-06-05	4.0	CVE-2018-2028 XF CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information. IBM X-Force ID: 155554.			FIRM
ibm -- control_desk	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565.	2019-06-05	4.0	CVE-2019-4056 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7.1 containers are vulnerable to privilege escalation due to an insecurely configured component. IBM X-Force ID: 158975.	2019-06-05	5.4	CVE-2019-4185 XF CONFIRM
icewarp -- mail_server	IceWarp Mail Server through 10.4.4 is prone to a local file inclusion vulnerability via webmail/calendar/minimizer/index.php?style=..%5c directory traversal.	2019-06-03	5.0	CVE-2019-12593 MISC MISC
ikiwiki -- ikiwiki	ikiwiki before 3.20170111.1 and 3.2018x and 3.2019x before 3.20190226 allows SSRF via the aggregate plugin. The impact also includes reading local files via file: URIs.	2019-06-05	5.0	CVE-2019-9187 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
istio -- istio	Istio 1.1.x through 1.1.6 has Incorrect Access Control.	2019-06-05	5.4	CVE-2019-12243 MISC CONFIRM
ivanti -- landesk_management_suite	Improper access control and open directories in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 may lead to remote disclosure of administrator passwords.	2019-06-03	5.0	CVE-2019-12373 MISC MISC
ivanti -- landesk_management_suite	A SQL Injection vulnerability exists in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 due to improper username sanitization in the Basic Authentication implementation in core/provisioning.secure/ProvisioningSecure.asmx in Provisioning.Secure.dll.	2019-06-03	6.8	CVE-2019-12374 MISC MISC
jenkins -- pipeline_maven_integration	An XML external entities (XXE) vulnerability in Jenkins Pipeline Maven Integration Plugin 1.7.0 and earlier allowed attackers able to control a temporary directory's	2019-05-31	5.5	CVE-2019-10327 MLIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	content on the agent running the Maven build to have Jenkins parse a maliciously crafted XML file that uses external entities for extraction of secrets from the Jenkins master, server-side request forgery, or denial-of-service attacks.			T BID MISC
jenkins -- pipeline_remote_loader	Jenkins Pipeline Remote Loader Plugin 1.4 and earlier provided a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection.	2019-05-31	6.5	CVE-2019-10328 MLIST BID MISC
jenkins -- warnings_next_generation	A cross-site request forgery vulnerability in Jenkins Warnings NG Plugin 5.0.0 and earlier allowed attackers to reset warning counts for future builds.	2019-05-31	4.3	CVE-2019-10326 MLIST BID MISC
jfrog -- artifactory	A cross-site request forgery vulnerability in Jenkins Artifactory Plugin 3.2.2 and earlier in ArtifactoryBuilder.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using	2019-05-31	4.3	CVE-2019-10321 MLIST BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.			MISC MISC
jfrog -- artifactory	A missing permission check in Jenkins Artifactory Plugin 3.2.2 and earlier in ArtifactoryBuilder.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-05-31	4.0	CVE-2019-10322 MLIST BID MISC MISC
jfrog -- artifactory	A missing permission check in Jenkins Artifactory Plugin 3.2.3 and earlier in various 'fillCredentialsIdItems' methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2019-05-31	4.0	CVE-2019-10323 MLIST BID MISC MISC
jfrog -- artifactory	A cross-site request forgery vulnerability in Jenkins Artifactory Plugin 3.2.2 and earlier in ReleaseAction#doSubmit, GradleReleaseApiAction#doStaging,	2019-05-31	4.3	CVE-2019-10324 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	MavenReleaseApiAction#doStaging, and UnifiedPromoteBuildAction#doSubmit allowed attackers to schedule a release build, perform release staging for Gradle and Maven projects, and promote previously staged builds, respectively.			BID MISC
malwarebytes -- antimalware	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Malwarebytes Antimalware 3.6.1.2711. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page. There is an issue with the way the product handles URIs within certain schemes. The product does not warn the user that a dangerous navigation is about to take place. Because special characters in the URI are not sanitized, this could lead to the execution of arbitrary commands. An attacker can leverage this vulnerability to execute code in the context of the current user at medium integrity. Was ZDI-CAN-7162.	2019-06-03	6.8	CVE-2019-6739 MISC
mantisbt -- mantisbt	An issue was discovered in MantisBT through 1.3.14, and 2.0.0. Using a crafted request on bug_report_page.php (modifying the 'm_id' parameter), any user with	2019-06-06	4.0	CVE-2018-9839 CONFIR

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	REPORTER access or above is able to view any private issue's details (summary, description, steps to reproduce, additional information) when cloning it. By checking the 'Copy issue notes' and 'Copy attachments' checkboxes and completing the clone operation, this data also becomes public (except private notes).			MMISC
marvell -- 88ss1074_firmware	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism.	2019-06-04	4.9	CVE-2019-10636 CONFIRM
mybb -- mybb	MyBB 1.8.19 has XSS in the resetpassword function.	2019-06-06	4.3	CVE-2019-3578 MISC CONFIRM
mybb -- mybb	MyBB 1.8.19 allows remote attackers to obtain sensitive information because it discloses the username upon receiving a	2019-06-06	5.0	CVE-2019-3579 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	password-reset request that lacks the code parameter.			CONFIRM
nvidia -- vibrante_linux	NVIDIA Vibrante Linux version 1.1, 2.0, and 2.2 contains a vulnerability in the user space driver in which protection mechanisms are insufficient, may lead to denial of service or information disclosure.	2019-06-05	4.6	CVE-2017-6261 MISC
otrs -- otrs	An issue was discovered in Open Ticket Request System (OTRS) 7.x before 7.0.5. An attacker who is logged into OTRS as an agent or a customer user can use the search result screens to disclose information from invalid system entities. Following is the list of affected entities: Custom Pages, FAQ Articles, Service Catalogue Items, ITSM Configuration Items.	2019-06-03	4.0	CVE-2019-9753 MISC
parso_project -- parso	A deserialization vulnerability exists in the way parso through 0.4.0 handles grammar parsing from the cache. Cache loading relies on pickle and, provided that an evil pickle can be written to a cache grammar file and that its parsing can be triggered, this flaw leads to Arbitrary Code Execution.	2019-06-06	6.0	CVE-2019-12760 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phome -- empirecms	admin\db\DoSql.php in EmpireCMS through 7.5 allows remote attackers to execute arbitrary PHP code via SQL injection that uses a .php filename in a SELECT INTO OUTFILE statement to admin/admin.php.	2019-06-07	6.5	CVE-2018-19462 MISC MISC MISC
phpmyadmin -- phpmyadmin	An issue was discovered in phpMyAdmin before 4.9.0. A vulnerability was found that allows an attacker to trigger a CSRF attack against a phpMyAdmin user. The attacker can trick the user, for instance through a broken <img> tag pointing at the victim's phpMyAdmin database, and the attacker can potentially deliver a payload (such as a specific INSERT or DELETE statement) to the victim.	2019-06-05	4.3	CVE-2019-12616 BID MISC CONFIRM
progress -- fiddler	Telerik Fiddler v5.0.20182.28034 doesn't verify the hash of EnableLoopback.exe before running it, which could lead to code execution or local privilege escalation by replacing the original EnableLoopback.exe.	2019-06-03	6.8	CVE-2019-12097 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pulsesecure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure (PCS) before 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4 and Pulse Policy Secure (PPS) before 5.1R15.1, 5.2 before 5.2R12.1, 5.3 before 5.3R15.1, 5.4 before 5.4R7.1, and 9.0 before 9.0R3.2, an authenticated attacker (via the admin web interface) can exploit Incorrect Access Control to execute arbitrary code on the appliance.	2019-06-03	6.5	CVE-2019-11509 MISC CONFIRM
pydio -- pydio	The "action" get_sess_id in the web application of Pydio through 8.2.2 discloses the session cookie value in the response body, enabling scripts to get access to its value. This identifier can be reused by an attacker to impersonate a user and perform actions on behalf of him/her (if the session is still active).	2019-05-31	6.4	CVE-2019-10045 MISC
pydio -- pydio	An unauthenticated attacker can obtain information about the Pydio 8.2.2 configuration including session timeout, libraries, and license information.	2019-05-31	5.0	CVE-2019-10046 MISC
pydio -- pydio	It is possible for an attacker with regular user access to the web application of Pydio through 8.2.2 to trick an administrator user into opening a link shared through the	2019-05-31	4.9	CVE-2019-10049

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application, that in turn opens a shared file that contains JavaScript code (that is executed in the context of the victim user to obtain sensitive information such as session identifiers and perform actions on behalf of him/her).			MISC
python -- pyxdg	A code injection issue was discovered in PyXDG before 0.26 via crafted Python code in a Category element of a Menu XML document in a .menu file. XDG_CONFIG_DIRS must be set up to trigger xdg.Menu.parse parsing within the directory containing this file. This is due to a lack of sanitization in xdg/Menu.py before an eval call.	2019-06-06	5.1	CVE-2019-12761 MISC MISC
redhat -- openstack	An access-control flaw was found in the Octavia service when the cloud platform was deployed using Red Hat OpenStack Platform Director. An attacker could cause new amphorae to run based on any arbitrary image. This meant that a remote attacker could upload a new amphorae image and, if requested to spawn new amphorae, Octavia would then pick up the compromised image.	2019-06-03	6.8	CVE-2019-3895 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redhat -- rkt	rkt through version 1.30.0 does not isolate processes in containers that are run with `rkt enter`. Processes run with `rkt enter` are given all capabilities during stage 2 (the actual environment in which the applications run). Compromised containers could exploit this flaw to access host resources.	2019-06-03	6.9	CVE-2019-10144 CONFIRM MISC
redhat -- rkt	rkt through version 1.30.0 does not isolate processes in containers that are run with `rkt enter`. Processes run with `rkt enter` do not have seccomp filtering during stage 2 (the actual environment in which the applications run). Compromised containers could exploit this flaw to access host resources.	2019-06-03	6.9	CVE-2019-10145 CONFIRM MISC
redhat -- rkt	rkt through version 1.30.0 does not isolate processes in containers that are run with `rkt enter`. Processes run with `rkt enter` are not limited by cgroups during stage 2 (the actual environment in which the applications run). Compromised containers could exploit this flaw to access host resources.	2019-06-03	6.9	CVE-2019-10147 CONFIRM MISC
saet -- webapp	The WebApp v04.68 in the supervisor on SAET Impianti Speciali TEBE Small 05.01 build 1137 devices allows remote attackers to make several types of	2019-05-31	5.0	CVE-2019-9105 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	API calls without authentication, as demonstrated by retrieving password hashes via an inc/utils/REST_API.php?command=CallAPI&customurl=alladminusers call.			MISC
sitecore -- cms	Deserialization of Untrusted Data in the anti CSRF module in Sitecore through 9.1 allows an authenticated attacker to execute arbitrary code by sending a serialized .NET object in an HTTP POST parameter.	2019-05-31	6.5	CVE-2019-9875 MISC MISC MISC
southrivertech -- titan_ftp_server	A Directory Traversal issue was discovered in the Web GUI in Titan FTP Server 2019 Build 3505. When an authenticated user attempts to preview an uploaded file (through PreviewHandler.ashx) by using a \..\..\ technique, arbitrary files can be loaded in the server response outside the root directory.	2019-06-03	4.0	CVE-2019-10009 MISC FULLDISC CONFIRM MISC EXPLOIT-DB EXP

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				LOIT -DB
sweetscape -- 010_editor	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the WSubStr function (provided by the scripting engine) allows an attacker to cause a denial of service by crashing the application.	2019 -06- 05	5.0	CVE- 2019- 1255 4 MIS C CON FIR M
sweetscape -- 010_editor	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the SubStr function (provided by the scripting engine) allows an attacker to cause a denial of service by crashing the application.	2019 -06- 05	5.0	CVE- 2019- 1255 5 MIS C CON FIR M
thehive-project -- thehive	An improper authorization check in the User API in TheHive before 2.13.4 and 3.x before 3.3.1 allows users with read-only or read/write access to escalate their privileges to the administrator's privileges. This affects app/controllers/UserCtrl.scala.	2019 -06- 02	6.5	CVE- 2017- 1837 6 MIS C MIS C

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tinycc -- tinycc	An issue was discovered in Tiny C Compiler (aka TinyCC or TCC) 0.9.27. Compiling a crafted source file leads to a one-byte out-of-bounds write in the gsym_addr function in x86_64-gen.c. This occurs because tccasm.c mishandles section switches.	2019-05-31	4.3	CVE-2019-12495 BID MISC MISC
tuxera -- ntfs-3g	An integer underflow issue exists in ntfs-3g 2017.3.23. A local attacker could potentially exploit this by running /bin/ntfs-3g with specially crafted arguments from a specially crafted directory to cause a heap buffer overflow, resulting in a crash or the ability to execute arbitrary code. In installations where /bin/ntfs-3g is a setuid-root binary, this could lead to a local escalation of privileges.	2019-06-05	4.4	CVE-2019-9755 MISC
vfront -- vfront	VFront 0.99.5 has stored XSS via the admin/sync_reg_tab.php azzera parameter, which is mishandled during admin/error_log.php rendering.	2019-06-03	4.3	CVE-2019-9838 MISC MISC
vfront -- vfront	VFront 0.99.5 has Reflected XSS via the admin/menu_registri.php descrizione_g parameter or the	2019-06-03	4.3	CVE-2019-9839 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	admin/sync_reg_tab.php azzera parameter.			CMISC
vtiger -- vtiger_crm	vtiger CRM 7.0.1 is affected by one reflected Cross-Site Scripting (XSS) vulnerability affecting version 7.0.1 and probably prior versions. This vulnerability could allow remote unauthenticated attackers to inject arbitrary web script or HTML via index.php?module=Contacts&view=List (app parameter).	2019-06-06	4.3	CVE-2018-8047 MISC
yubico -- pam-u2f	Yubico pam-u2f 1.0.7 attempts parsing of the configured authfile (default $HOME/.config/Yubico/u2f_keys) as root (unless openasuser was enabled), and does not properly verify that the path lacks symlinks pointing to other files on the system owned by root. If the debug option is enabled in the PAM configuration, part of the file contents of a symlink target will be logged, possibly revealing sensitive information.	2019-06-04	5.0	CVE-2019-12209 MLIST CONFIRM CONFIRM
yubico -- pam-u2f	In Yubico pam-u2f 1.0.7, when configured with debug and a custom debug log file is set using debug_file, that file descriptor is not closed when a new process is spawned. This leads to the file	2019-06-04	5.5	CVE-2019-12210 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	descriptor being inherited into the child process; the child process can then read from and write to it. This can leak sensitive information and also, if written to, be used to fill the disk or plant misinformation.			CONFIRM CONFIRM
zohocorp -- manageengine_servicedesk_plus	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the SiteLookup.do search field.	2019-06-05	4.3	CVE-2019-12538 MISC MISC
zohocorp -- manageengine_servicedesk_plus	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the SolutionSearch.do searchText parameter.	2019-06-05	4.3	CVE-2019-12541 MISC MISC
zohocorp -- manageengine_servicedesk_plus	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the SearchN.do userConfigID parameter.	2019-06-05	4.3	CVE-2019-12542 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zohocorp -- manageengine_servicedesk_plus	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the PurchaseRequest.do serviceRequestId parameter.	2019-06-05	4.3	CVE-2019-12543 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chartered_accountant_:_auditor_website_project -- chartered_accountant_:_auditor_website	PHP Scripts Mall Chartered Accountant : Auditor Website 2.0.1 has Stored XSS in the Profile Update page via the My Name field.	2019-06-06	3.5	CVE-2019-7553 MISC MISC
cisco -- industrial_network_director	A vulnerability in Cisco Industrial Network	2019-06-05	3.5	CVE-2019-1882

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Director could allow an authenticated, remote attacker to conduct stored cross-site scripting (XSS) attacks. The vulnerability is due to improper validation of content submitted to the affected application. An attacker could exploit this vulnerability by sending requests containing malicious values to the affected system. A successful exploit could allow the attacker to conduct XSS attacks.			BID CISCO
cmsmadesimple -- cms_made_simple	CMS Made Simple 2.2.10 has XSS via the m1_name	2019-06-05	3.5	CVE-2019-11226 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter in "Add Article" under Content -> Content Manager -> News.			FULLDISC MISC
ibm -- infosphere_information_server_on_cloud	IBM InfoSphere Information Server 11.7.1.0 stores a common hard coded encryption key that could be used to decrypt sensitive information. IBM X-Force ID: 159229.	2019-06-05	2.1	CVE-2019-4220 XF CONFIRM
investment_mlm_project -- investment_mlm	An issue was discovered in PHP Scripts Mall Investment MLM Software 2.0.2. Stored XSS was found in the the My Profile Section. This is due to lack of sanitization in the Edit Name section.	2019-06-06	3.5	CVE-2019-7552 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ivanti -- landesk_management_suite	Use of a hard-coded encryption key in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 may lead to full managed endpoint compromise by an authenticated user with read privileges.	2019-06-03	3.5	CVE-2019-12376 MISC
jenkins -- warnings_next_generation	A cross-site scripting vulnerability in Jenkins Warnings NG Plugin 5.0.0 and earlier allowed attacker with Job/Configure permission to inject arbitrary JavaScript in build overview pages.	2019-05-31	3.5	CVE-2019-10325 MLIST BID MISC
liferay -- liferay_portal	In Liferay Portal before	2019-06-03	2.6	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	7.1 CE GA4, an XSS vulnerability exists in the SimpleCaptcha API when custom code passes unsanitized input into the "url" parameter of the JSP taglib call <liferay-ui:captcha url="<%= url %>" /> or <liferay-captcha:captcha url="<%= url %>" />. Liferay Portal out-of-the-box behavior with no customizations is not vulnerable.			6588 CONFIRM
marvell -- 88ss1074_firmware	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174,	2019-06-05	2.1	CVE-2019-10637 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism.			
phome -- empirecms	admin\db\DoSql.php in EmpireCMS through 7.5 allows XSS via crafted SQL syntax to admin/admin.php.	2019-06-07	3.5	CVE-2018-19461 MISC MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices allow Authenticated Stored XSS.	2019-06-05	3.5	CVE-2019-7671 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pydio -- pydio	A stored XSS vulnerability exists in the web application of Pydio through 8.2.2 that can be exploited by levering the file upload and file preview features of the application. An authenticated attacker can upload an HTML file containing JavaScript code and afterwards a file preview URL can be used to access the uploaded file. If a malicious user shares an uploaded HTML file containing JavaScript code with another user of the application, and tricks an authenticated victim into accessing a	2019-05-31	3.5	CVE-2019-10047 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	URL that results in the HTML code being interpreted by the web browser, then the included JavaScript code is executed under the context of the victim user session.			
qemu -- qemu	tcp_emu in slirp/tcp_subr.c (aka slirp/src/tcp_subr.c) in QEMU 3.0.0 uses uninitialized data in an snprintf call, leading to Information disclosure.	2019-06-03	2.1	CVE-2019-9824 MISC
schneider-electric -- citectscada	In Vijeo Citect 7.30 and 7.40, and CitectSCADA 7.30 and 7.40, a vulnerability has been identified that may allow an authenticated	2019-05-31	2.1	CVE-2019-10981 BID MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	local user access to Citect user credentials.			
veronalabs -- wp_statistics	The WP Statistics plugin through 12.6.5 for Wordpress has stored XSS in includes/class-wp-statistics-pages.php. This is related to an account with the Editor role creating a post with a title that contains JavaScript, to attack an admin user.	2019-06-02	3.5	CVE-2019-12566 MISC MISC MISC

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
anviz -- m3_outdoor_rfid_access_control	Anviz Global M3 Outdoor RFID Access Control executes any command received from any source. No authentication/encryption is done. Attackers can fully interact with the device: for example, send the "open door" command, download the users list (which includes RFID codes and passcodes in cleartext), or update/create users. The same attack can be executed on a local network and over the internet (if the device is exposed on a public IP address).	2019-06-06	not yet calculated	CVE-2019-11523 MISC
au_optronics -- data_recorder	Stored XSS was discovered in AUO Solar Data Recorder before 1.3.0 via the protect/config.htm addr parameter.	2019-06-03	not yet calculated	CVE-2019-11368 MISC MISC
au_optronics -- data_recorder	An issue was discovered in AUO Solar Data Recorder before 1.3.0. The web portal uses HTTP Basic Authentication and provides the account and password in the	2019-06	not yet	CVE-20

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WWW-Authenticate attribute. By using this account and password, anyone can login successfully.	-03	calculated	19-11367 MISC MISC MISC
carel_industries -- pcoweb	An issue was discovered in Carel pCOWeb prior to B1.2.4. In /config/pw_changeusers.html the device stores cleartext passwords, which may allow sensitive information to be read by someone with access to the device.	2019-06-03	not yet calculated	CVE-2019-11369 MISC MISC
carel_industries -- pcoweb	Stored XSS was discovered in Carel pCOWeb prior to B1.2.4, as demonstrated	2019	not	CV

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by the config/pw_snmp.html "System contact" field.	-06-03	yet calculated	E-2019-11370 MISC MISC
chartkick_gem_for_ruby_on_rails -- chartkick_gem_for_ruby_on_rails	The Chartkick gem through 3.1.0 for Ruby allows XSS.	2019-06-06	not yet calculated	CVE-2019-12732 CONFIRM CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM
cisco -- industrial_network_director	A vulnerability in the software update feature of Cisco Industrial Network Director could allow an authenticated, remote attacker to execute arbitrary code. The vulnerability is due to improper validation of files uploaded to the affected application. An attacker could exploit this vulnerability by authenticating to the affected system using administrator privileges and uploading an arbitrary file. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges.	2019-06-05	not yet calculated	CVE-2019-1861 BID CISCO
cisco -- unified_computing_system_c-series_rack_servers	A vulnerability in the BIOS upgrade utility of Cisco Unified Computing System (UCS) C-Series Rack Servers could allow an authenticated, local attacker to install compromised BIOS firmware on an affected device. The vulnerability is due to insufficient validation of the firmware image file. An attacker could exploit this vulnerability by executing the BIOS upgrade utility with a specific set of options. A successful exploit could allow the attacker to bypass the firmware signature-verification process and install compromised BIOS firmware on an affected device.	2019-06-05	not yet calculated	CVE-2019-1880 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
citrix -- application_delivery_management	Citrix Application Delivery Management (ADM) 12.1.x before 12.1.50.33 has Incorrect Access Control.	2019-06-05	not yet calculated	CVE-2019-9548 CONFIRM MISC
citrix -- sd-wan_center_and_netscaler_sd-wan_center	Citrix SD-WAN Center 10.2.x before 10.2.1 and NetScaler SD-WAN Center 10.0.x before 10.0.7 allow Command Injection.	2019-06-03	not yet calculated	CVE-2019-10883 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC MISC
cloudera -- data_science_workbench	An SQL injection vulnerability was found in Cloudera Data Science Workbench (CDSW) 1.4.0 through 1.4.2. This would allow any authenticated user to run arbitrary queries against CDSW's internal database. The database contains user contact information, encrypted CDSW passwords (in the case of local authentication), API keys, and stored Kerberos keytabs.	2019-06-07	not yet calculated	CVE-2018-20091 CONFIRM MISC
cloudera -- navigator_key_trustee_kms	In Cloudera Navigator Key Trustee KMS 5.12 and 5.13, incorrect default ACL values allow remote access to purge and undelete API calls on encryption zone	2019-06	not yet	CVE-20

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	keys. The Navigator Key Trustee KMS includes 2 API calls in addition to those in Apache Hadoop KMS: purge and undelete. The KMS ACL values for these commands are keytrustee.kms.acl.PURGE and keytrustee.kms.acl.UNDELETE respectively. The default value for the ACLs in Key Trustee KMS 5.12.0 and 5.13.0 is "*" which allows anyone with knowledge of the name of an encryption zone key and network access to the Key Trustee KMS to make those calls against known encryption zone keys. This can result in the recovery of a previously deleted, but not purged, key (undelete) or the deletion of a key in active use (purge) resulting in loss of access to encrypted HDFS data.	-07	calculated	18-6185 MISCCONFIRM
clusterlabs -- libqb	libqb before 1.0.5 allows local users to overwrite arbitrary files via a symlink attack, because it uses predictable filenames (under /dev/shm and /tmp) without O_EXCL.	2019-06-07	not yet calculated	CVE-2019-12779 MISCMIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CMISCMISC
dameware -- dameware_remote_mini_control	Dameware Remote Mini Control version 12.1.0.34 and prior contains a unauthenticated remote heap overflow due to the server not properly validating RsaPubKeyLen during key negotiation. An unauthenticated remote attacker can cause a heap buffer overflow by specifying a large RsaPubKeyLen, which could cause a denial of service.	2019-06-07	not yet calculated	CVE-2019-3955 MISC
dell_emc -- openmanage_server_administrator	Dell EMC OpenManage Server Administrator (OMSA) versions prior to 9.1.0.3 and prior to 9.2.0.4 contain a web parameter tampering vulnerability. A remote unauthenticated attacker could potentially manipulate parameters of web requests to OMSA to create arbitrary files with empty content or delete the contents of any existing file, due to improper input parameter validation	2019-06-06	not yet calculated	CVE-2019-3723 BID CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				FIRM
dell_emc -- openmanage_server_administrator	Dell EMC OpenManage Server Administrator (OMSA) versions prior to 9.1.0.3 and prior to 9.2.0.4 contain an XML external entity (XXE) injection vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to read arbitrary server system files by supplying specially crafted document type definitions (DTDs) in an XML request.	2019-06-06	not yet calculated	CVE-2019-3722 BID CONFIRM
digitaldruid.net -- hoteldruid	In Hoteldruid before 2.3.1, a division by zero was discovered in $num_tabelle in tab_tariffe.php (aka the numtariffa1 parameter) due to the mishandling of non-numeric values, as demonstrated by the /tab_tariffe.php?anno=[YEAR]&numtariffa1=1a URI. It could allow an administrator to conduct remote denial of service (disrupting certain business functions of the product).	2019-06-07	not yet calculated	CVE-2019-9084 MISC M

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ISC
enttec -- datagate_mk2	A number of stored XSS vulnerabilities have been identified in the web configuration feature in ENTTEC Datagate Mk2 70044_update_05032019-482 that could allow an unauthenticated threat actor to inject malicious code directly into the application. This affects, for example, the Profile Description field in JSON data to the Profile Editor.	2019-06-07	not yet calculated	CVE-2019-12774 MISC
enttec -- multiple_products	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They include a hard-coded SSH backdoor for remote SSH and SCP access as the root user. A command in the relocate and relocate_revB scripts copies the hardcoded key to the root user's authorized_keys file, enabling anyone with the associated private key to gain remote root access to all affected products.	2019-06-07	not yet calculated	CVE-2019-12776 MISC
enttec -- multiple_products	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware	2019-	not ye	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	70044_update_05032019-482. They replace secure and protected directory permissions (set as default by the underlying operating system) with highly insecure read, write, and execute directory permissions for all users. By default, /usr/local and all of its subdirectories should have permissions set to only allow non-privileged users to read and execute from the tree structure, and to deny users from creating or editing files in this location. The ENTTEC firmware startup script permits all users to read, write, and execute (rwxrwxrwx) from the /usr, /usr/local, /usr/local/dmxis, and /usr/local/bin/ directories.	06-07	tcalculated	2019-12777 MISC
enttec -- multiple_products	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They allow high-privileged root access by www-data via sudo without requiring appropriate access control. (Furthermore, the user account that controls the web application service is granted full access to run any system commands with elevated privilege, without the need for password authentication. Should vulnerabilities be identified and exploited within the web application, it may be possible for a threat actor to create or run high-privileged	2019-06-07	notyetcalculated	CVE-2019-12775 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	binaries or executables that are available within the operating system of the device.)			
foxit_software -- reader	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when using the Open File action on a Field. An attacker can leverage this to gain remote code execution.	2019-06-07	not yet calculated	CVE-2018-19451 MISC
foxit_software -- reader	A use after free in the TextBox field Mouse Enter action in IReader_ContentProvider can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031. An attacker can leverage this to gain remote code execution. Relative to CVE-2018-19444, this has a different free location and requires different JavaScript code for exploitation.	2019-06-07	not yet calculated	CVE-2018-19452 MISC
freenet -- freenet	Freenet 1483 has a MIME type bypass that allows arbitrary JavaScript execution via a crafted Freenet URI.	2019-	not ye	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
		06-05	t calculated	2019-9673 MISCMISC
gallagher -- command_centre	Gallagher Command Centre before 7.80.939, 7.90.x before 7.90.961, and 8.x before 8.00.1128 allows arbitrary event creation and information disclosure via the FT Command Centre Service and FT Controller Service services.	2019-06-06	not yet calculated	CVE-2019-12492 CONFIRM CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				FIRM
gemalto -- admin_control_center	Gemalto Admin Control Center, all versions prior to 7.92, uses cleartext HTTP to communicate with www3.safenet-inc.com to obtain language packs. This allows attacker to do man-in-the-middle (MITM) attack and replace original language pack by malicious one.	2019-06-07	not yet calculated	CVE-2019-8282 MISC
gemalto -- admin_control_center	Hasplm cookie in Gemalto Admin Control Center, all versions prior to 7.92, does not have 'HttpOnly' flag. This allows malicious javascript to steal it.	2019-06-07	not yet calculated	CVE-2019-8283 MISC
gemalto -- ds3_authentication_server	Gemalto DS3 Authentication Server 2.6.1-SP01 has Broken Access Control.	2019-06	not yet	CVE-20

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
		-05	calculated	19-9158 MISC MISC
gemalto -- ds3_authentication_server	Gemalto DS3 Authentication Server 2.6.1-SP01 allows Local File Disclosure.	2019-06-05	not yet calculated	CVE-2019-9157 MISC MISC
gemalto -- ds3_authentication_server	Gemalto DS3 Authentication Server 2.6.1-SP01 allows OS Command Injection.	2019-06-05	not yet calcul	CVE-2019-91

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			ated	56 MISC MISC
google -- android	In callGenIDChangeListeners and related functions of SkPixelRef.cpp, there is a possible use after free due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-124232283.	2019-06-07	not yet calculated	CVE-2019-2095 CONFIRM
google -- android	In uvc_parse_standard_control of uvc_driver.c, there is a possible out-of-bound read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-111760968.	2019-06-07	not yet calculated	CVE-2019-2101 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
google -- android	In parseMPEGCCData of NuPlayerCCDecoder.cpp, there is a possible out of bounds write due to missing bounds checks. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-129068792.	2019-06-07	not yet calculated	CVE-2019-2094 CONFIRM
google -- android	In the Bluetooth Low Energy (BLE) specification, there is a provided example Long Term Key (LTK). If a BLE device were to use this as a hardcoded LTK, it is theoretically possible for a proximate attacker to remotely inject keystrokes on a paired Android host due to improperly used crypto. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128843052.	2019-06-07	not yet calculated	CVE-2019-2102 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM
google -- android	In isSeparateProfileChallengeAllowed of DevicePolicyManagerService.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege, with no additional permissions required. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128599668.	2019-06-07	not yet calculated	CVE-2019-2092 CONFIRM
google -- android	In nfa_rw_store_ndef_rx_buf of nfa_rw_act.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-123583388.	2019-06-07	not yet calculated	CVE-2019-2099 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In areNotificationsEnabledForPackage of NotificationManagerService.java, there is a possible permissions bypass due to a missing permissions check. This could lead to local escalation of privilege, with no additional privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128599467.	2019-06-07	not yet calculated	CVE-2019-2098 CONFIRM
google -- android	In HAliasAnalyzer.Query of hydrogen-alias-analysis.h, there is possible memory corruption due to type confusion. This could lead to remote code execution from a malicious proxy configuration, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-117606285.	2019-06-07	not yet calculated	CVE-2019-2097 CONFIRM
google -- android	In GetPermittedAccessibilityServicesForUser of DevicePolicyManagerService.java, there	2019-	not ye	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege, with no additional permissions required. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1. Android ID: A-128599660.	06-07	t calculated	2019-2091 CONFIRM
google -- android	In huff_dec_1D of nlc_dec.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-119292397.	2019-06-07	not yet calculated	CVE-2019-2093 CONFIRM
google -- android	In EffectRelease of EffectBundle.cpp, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for	2019-06-07	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-123237974.		ulated	2096 CONFIRM
google -- android	In isPackageDeviceAdminOnAnyUser of PackageManagerService.java, there is a possible permissions bypass due to a missing permissions check. This could lead to local escalation of privilege, with no additional permissions required. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128599183	2019-06-07	not yet calculated	CVE-2019-2090 CONFIRM
hapi_fhir -- hapi_fhir	XSS exists in the HAPI FHIR testpage overlay module of the HAPI FHIR library before 3.8.0. The attack involves unsanitized HTTP parameters being output in a form page, allowing attackers to leak cookies and other sensitive information from ca/uhn/fhir/to/BaseController.java via a specially crafted URL. (This module is not generally used in production systems	2019-06-05	not yet calculated	CVE-2019-12741

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	so the attack surface is expected to be low, but affected systems are recommended to upgrade immediately.)			MISC MISC MISC
hashicorp -- consul	HashiCorp Consul 1.4.0 through 1.5.0 has Incorrect Access Control. Keys not matching a specific ACL rule used for prefix matching in a policy can be deleted by a token using that policy even with default deny settings configured.	2019-06-06	not yet calculated	CVE-2019-12291 CONFIRM
hewlett_packard_enterprise -- integrated_maintenance_entity_and_maintenance_entity_and_blade_maintenance_entity	The HPE Nonstop Maintenance Entity family of products are vulnerable to local disclosure of information, such as system layout and configuration.	2019-06-05	not yet calcul	CVE-2019-53

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			ated	94 CONFIRM
hewlett_packard_enterprise -- smart_update_manager	A security vulnerability in HPE Smart Update Manager (SUM) prior to v8.4 could allow local unauthorized elevation of privilege.	2019-06-05	not yet calculated	CVE-2019-11987 CONFIRM
hewlett_packard_enterprise -- smart_update_manager	A Remote Unauthorized Access vulnerability was identified in HPE Smart Update Manager (SUM) earlier than version 8.3.5.	2019-06-05	not yet calculated	CVE-2019-11988

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
hgiga -- oaklouds_mailsherlock	Multi modules of MailSherlock MSR35 and MSR45 lead to a CSRF vulnerability. It allows attacker to add malicious email sources into whitelist via user/save_list.php?ACSION=&type=email&category=white&locate=big5&cmd=add&new=hacker@socialengineering.com&new_memo=&add=%E6%96%B0%E5%A2%9E without any authorizes.	2019-06-03	not yet calculated	CVE-2019-9882 MISC MISC
hgiga -- oaklouds_mailsherlock	Multi modules of MailSherlock MSR35 and MSR45 lead to a CSRF vulnerability. It allows attacker to elevate privilege of specific account via useradmin/cf_new.cgi?chief=&wk_group=full&cf_name=test&cf_account=test&cf_email=&cf_acl=Management&apply_lang=&dn= without any authorizes.	2019-06-03	not yet calculated	CVE-2019-9883 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
htc_corporation -- viveport	Privilege escalation due to insecure directory permissions affecting ViveportDesktopService in HTC VIVEPORT before 1.0.0.36 allows local attackers to escalate privileges via DLL hijacking.	2019-06-03	not yet calculated	CVE-2019-12177 MISC MISC MISC
htc_corporation -- viveport	Privilege escalation in the "HTC Account Service" and "ViveportDesktopService" in HTC VIVEPORT before 1.0.0.36 allows local attackers to escalate privileges to SYSTEM via reconfiguration of either service.	2019-06-03	not yet calculated	CVE-2019-12176 M

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ISCMISC
huawei -- ap_products	There is an improper authentication vulnerability in some Huawei AP products before version V200R009C00SPC800. Due to the improper implementation of authentication for the serial port, an attacker could exploit this vulnerability by connecting to the affected products and running a series of commands.	2019-06-04	not yet calculated	CVE-2019-5298 CONFIRM
huawei -- mate_10_smartphones	The image processing module of some Huawei Mate 10 smartphones versions before ALP-L29 9.0.0.159(C185) has a memory double free vulnerability. An attacker tricks a user into installing a malicious application, and the application can call special API, which could trigger double free and cause a system crash.	2019-06-06	not yet calculated	CVE-2019-5305 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM
huawei -- p20_smartphones	There is a Factory Reset Protection (FRP) bypass security vulnerability in P20 Huawei smart phones versions before Emily-AL00A 9.0.0.167(C00E81R1P21T8). When re-configuring the mobile phone using the FRP function, an attacker can delete the activation lock after a series of operations. As a result, the FRP function is bypassed and the attacker gains access to the smartphone.	2019-06-04	not yet calculated	CVE-2019-5306 CONFIRM
huawei -- emily-l29c_smartphones	Emily-L29C Huawei phones versions earlier than 9.0.0.159 (C185E2R1P12T8) have a Factory Reset Protection (FRP) bypass security vulnerability. Before the FRP account is verified and activated during the reset process, the attacker can perform some special operations to bypass the FRP function and obtain the right to use the mobile phone.	2019-06-04	not yet calculated	CVE-2019-5297 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones versions earlier than Berkeley-AL20 9.0.0.125(C00E125R2P14T8) have an authorization bypass vulnerability. Due to improper authorization implementation logic, attackers can bypass certain authorization scopes of smart phones by performing specific operations. This vulnerability can be exploited to perform operations beyond the scope of authorization.	2019-06-06	not yet calculated	CVE-2019-5295 CONFIRM
huawei -- leland_al00a_smartphones	There is a DoS vulnerability in RTSP module of Leland-AL00A Huawei smart phones versions earlier than Leland-AL00A 9.1.0.111(C00E111R2P10T8). Remote attackers could trick the user into opening a malformed RTSP media stream to exploit this vulnerability. Successful exploit could cause the affected phone abnormal, leading to a DoS condition. (Vulnerability ID: HWPSIRT-2019-02004)	2019-06-04	not yet calculated	CVE-2019-5284 CONFIRM
huawei -- mate10_smartphones	There is a double free vulnerability on certain drivers of Huawei Mate10 smartphones versions earlier than ALP-	2019-	not ye	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	AL00B 9.0.0.181(C00E87R2P20T8). An attacker tricks the user into installing a malicious application, which makes multiple processes operate the same resource at the same time. Successful exploit could cause a denial of service condition.	06-06	t calculated	2019-5219 CONFIRM
huawei -- mate10_smartphones	There is a use after free vulnerability on certain driver component in Huawei Mate10 smartphones versions earlier than ALP-AL00B 9.0.0.167(C00E85R2P20T8). An attacker tricks the user into installing a malicious application, which make the software to reference memory after it has been freed. Successful exploit could cause a denial of service condition.	2019-06-06	not yet calculated	CVE-2019-5214 CONFIRM
huawei -- mate20_smartphones	Mate20 Huawei smartphones versions earlier than HMA-AL00C00B175 have an out-of-bounds read vulnerability. An attacker with a high permission runs some specific commands on the smartphone. Due to insufficient input verification,	2019-06-04	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	successful exploit may cause out-of-bounds read of the memory and the system abnormal.		ulated	5296 CONFIRM
huawei -- p20_smartphones	There is Factory Reset Protection (FRP) bypass security vulnerability in P20 Huawei smart phones versions earlier than Emily-AL00A 9.0.0.167 (C00E81R1P21T8). When re-configuring the mobile phone using the factory reset protection (FRP) function, an attacker can login the Talkback mode and can perform some operations to access the setting page. As a result, the FRP function is bypassed.	2019-06-04	not yet calculated	CVE-2019-5283 CONFIRM
huawei -- p30_smartphones	There is a man-in-the-middle (MITM) vulnerability on Huawei P30 smartphones versions before ELE-AL00 9.1.0.162(C01E160R1P12/C01E160R2P1), and P30 Pro versions before VOG-AL00 9.1.0.162 (C01E160R1P12/C01E160R2P1). When users establish connection and transfer data through Huawei Share, an attacker could	2019-06-04	not yet calculated	CVE-2019-5215 C

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sniff, spoof and do a series of operations to intrude the Huawei Share connection and launch a man-in-the-middle attack to obtain and tamper the data. (Vulnerability ID: HWPSIRT-2019-03109)			ONFIRM
huawei -- p30_and_p30_pro_4g_lte_devices	Some Huawei 4G LTE devices, P30 versions before ELE-AL00 9.1.0.162(C01E160R1P12/C01E160R2P1) and P30 Pro versions before VOG-AL00 9.1.0.162(C01E160R1P12/C01E160R2P1), are exposed to a message replay vulnerability. For the sake of better compatibility, these devices implement a less strict check on the NAS message sequence number (SN), specifically NAS COUNT. As a result, an attacker can construct a rogue base station and replay the GUTI reallocation command message in certain conditions to tamper with GUTIs, or replay the Identity request message to obtain IMSIs. (Vulnerability ID: HWPSIRT-2019-04107)	2019-06-04	not yet calculated	CVE-2019-5307 CONFIRM
huawei -- pcmanager	There is a privilege escalation vulnerability in Huawei PCManager versions earlier than PCManager 9.0.1.50. The attacker can tricking a user to install and run a malicious application to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	2019-06-06	not yet calculated	CVE-2019-5241 C

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
huawei -- pcmanager	There is a code execution vulnerability in Huawei PCManager versions earlier than PCManager 9.0.1.50. The attacker can tricking a user to install and run a malicious application to exploit this vulnerability. Successful exploitation may cause the attacker to execute malicious code and read/write memory.	2019-06-06	not yet calculated	CVE-2019-5242 CONFIRM
huawei -- y9_2019_smartphones	There is an information leak vulnerability in some Huawei phones, versions earlier than Jackman-L21 8.2.0.155(C185R1P2). When a local attacker uses the camera of a smartphone, the attacker can exploit this vulnerability to obtain sensitive information by performing a series of operations.	2019-06-04	not yet calculated	CVE-2019-5281 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM
huawei -- honor_v10_smartphones	There is a race condition vulnerability on Huawei Honor V10 smartphones versions earlier than Berkeley-AL20 9.0.0.156(C00E156R2P14T8), Honor 10 smartphones versions earlier than Columbia-AL10B 9.0.0.156(C00E156R1P20T8) and Honor Play smartphones versions earlier than Cornell-AL00A 9.0.0.156(C00E156R1P13T8). An attacker tricks the user into installing a malicious application, which makes multiple processes to operate the same variate at the same time. Successful exploit could cause execution of malicious code.	2019-06-06	not yet calculated	CVE-2019-52516 CONFIRM
huawei -- mate_9_pro_smartphones	Mate 9 Pro Huawei smartphones earlier than LON-L29C 8.0.0.361(C636) versions have an information leak vulnerability due to the lack of input validation. An attacker tricks the user who has root privilege to install an application on the smart phone, and the application can read some process information, which may cause sensitive information leak.	2019-06-04	not yet calculated	CVE-2019-52444 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- mate_9_pro_smartphones	There is an information disclosure vulnerability on Mate 9 Pro Huawei smartphones versions earlier than LON-AL00B9.0.1.150 (C00E61R1P8T8). An attacker could view the photos after a series of operations without unlocking the screen lock. Successful exploit could cause an information disclosure condition.	2019-06-04	not yet calculated	CVE-2019-5217 CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.5 and 11.7 is affected by an information disclosure vulnerability. Sensitive information in an error message may be used to conduct further attacks against the system. IBM X-Force ID: 159945.	2019-06-06	not yet calculated	CVE-2019-4257 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- intelligent_operations_center	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157015.	2019-06-07	not yet calculated	CVE-2019-4070 XFCONFIRM
ibm -- intelligent_operations_center	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 does not properly validate file types, allowing an attacker to upload malicious content. IBM X-Force ID: 157014.	2019-06-07	not yet calculated	CVE-2019-4069 XFCONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- intelligent_operations_center	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 is vulnerable to user enumeration, allowing an attacker to brute force into the system. IBM X-Force ID: 157013.	2019-06-07	not yet calculated	CVE-2019-4068 XFCONFIRM
ibm -- intelligent_operations_center	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 157012.	2019-06-07	not yet calculated	CVE-2019-4067 XFCONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- intelligent_operations_center	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 could allow an authenciated user to create arbitrary users which could cause ID management issues and result in code execution. IBM X-Force ID: 157011.	2019-06-07	not yet calculated	CVE-2019-4066 XFCONFIRM
ibm -- jazz_for_serivce_management	IBM Jazz for Service Management 1.1.3, 1.1.3.1, and 1.1.3.2 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 159122.	2019-06-05	not yet calculated	CVE-2019-4201 XFCONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311.	2019-06-05	not yet calculated	CVE-2019-4048 XFCONFIRM
ibm -- security_information_queue	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 is missing the HTTP Strict Transport Security header. Users can navigate by mistake to the unencrypted version of the web application or accept invalid certificates. This leads to sensitive data being sent unencrypted over the wire. IBM X-Force ID: 158661.	2019-06-06	not yet calculated	CVE-2019-4162 XFCONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_information_queue	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 159227.	2019-06-06	not yet calculated	CVE-2019-4218 XFCONFIRM
ibm -- security_information_queue	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 159228.	2019-06-06	not yet calculated	CVE-2019-4219 XFCONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_information_queue	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 158660.	2019-06-06	not yet calculated	CVE-2019-4161 XFCONFIRM
ibm -- security_information_queue	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 159226.	2019-06-06	not yet calculated	CVE-2019-4217 XFCONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
inateck -- wp1001_wireless_presenter	Due to unencrypted and unauthenticated data communication, the wireless presenter Inateck WP1001 v1.3C is prone to keystroke injection attacks. Thus, an attacker is able to send arbitrary keystrokes to a victim's computer system, e.g., to install malware when the target system is unattended. In this way, an attacker can remotely take control over the victim's computer that is operated with an affected receiver of this device.	2019-06-07	not yet calculated	CVE-2019-12505 MISC BUGTRAQ MISC
inateck -- wp2002_wireless_presenter	Due to unencrypted and unauthenticated data communication, the wireless presenter Inateck WP2002 is prone to keystroke injection attacks. Thus, an attacker is able to send arbitrary keystrokes to a victim's computer system, e.g., to install malware when the target system is unattended. In this way, an attacker can remotely take control over the victim's computer that is	2019-06-07	not yet calculated	CVE-2019-12504 M

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	operated with an affected receiver of this device.			ISCBUGTRAQMISC
kyocera -- command_center_rx	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.	2019-06-06	not yet calculated	CVE-2019-6452MISCMISC
logitech -- r700_laser_presentation_remote	Due to unencrypted and unauthenticated data communication, the wireless presenter Logitech R700 Laser Presentation Remote R-R0010 is prone to keystroke injection attacks. Thus, an attacker is able to send	2019-06	not yet ca	CVE-2019

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary keystrokes to a victim's computer system, e.g., to install malware when the target system is unattended. In this way, an attacker can remotely take control over the victim's computer that is operated with an affected receiver of this device.	-07	lcul ated	-12506 MISCBUGTRAQMISC
maccms -- maccms	Maccms through 8.0 allows XSS via the site_keywords field to index.php?m=system-config because of tpl/module/system.php and tpl/html/system_config.html, related to template/paody/html/vod_index.html.	2019-06-07	not yet calculated	CVE-2018-19465 MISCMISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
martin_raiber -- urbackup	In UrBackup 2.2.6, an attacker can send a malformed request to the client over the network, and trigger a fileservplugin/CClientThread.cpp CClientThread::GetFileHashAndMetadata NULL pointer dereference, leading to shutting down the client application.	2019-06-07	not yet calculated	CVE-2018-20014 MISC MISC
micro_focus -- solution_business_manager	Micro Focus Solution Business Manager versions prior to 11.4.2 is susceptible to open redirect.	2019-06-07	not yet calculated	CVE-2019-3477 CONFIRM
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. The device by default	2019	not	CV

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows HTTP traffic thus providing an insecure communication mechanism for a user connecting to the web server. This allows an attacker to sniff the traffic easily and allows an attacker to compromise sensitive data such as credentials.	-06-07	yet calculated	E-2018-10690 MISCBUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. It is intended that an administrator can download /systemlog.log (the system log). However, the same functionality allows an attacker to download the file without any authentication or authorization.	2019-06-07	not yet calculated	CVE-2018-10691 MISCBUG

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				TRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. The session cookie "Password508" does not have an HttpOnly flag. This allows an attacker who is able to execute a cross-site scripting attack to steal the cookie very easily.	2019-06-07	not yet calculated	CVE-2018-10692 MISCBUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides ping functionality so that an administrator can execute ICMP calls to check if the network is working correctly. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "srvName" is susceptible to a	2019-06-07	not yet calcul	CVE-2018-1069

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	buffer overflow. By crafting a packet that contains a string of 516 characters, it is possible for an attacker to execute the attack.		ated	3MISCBUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. The device provides a Wi-Fi connection that is open and does not use any encryption mechanism by default. An administrator who uses the open wireless connection to set up the device can allow an attacker to sniff the traffic passing between the user's computer and the device. This can allow an attacker to steal the credentials passing over the HTTP connection as well as TELNET traffic. Also an attacker can MITM the response and infect a user's computer very easily as well.	2019-06-07	not yet calculated	CVE-2018-10694 MISCBUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides alert functionality so that an administrator can send emails to his/her account when there are changes to the device's network. However, the same functionality allows an attacker to execute commands on the device. The POST parameters "to1,to2,to3,to4" are all susceptible to buffer overflow. By crafting a packet that contains a string of 678 characters, it is possible for an attacker to execute the attack.	2019-06-07	not yet calculated	CVE-2018-10695 MISC BUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. The device provides a web interface to allow an administrator to manage the device. However, this interface is not protected against CSRF attacks, which allows an attacker to trick an administrator into executing actions without his/her knowledge, as demonstrated by the forms/iw_webSetParameters and forms/webSetMainRestart URIs.	2019-06-07	not yet calculated	CVE-2018-10696 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				UGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. The Moxa AWK 3121 provides certfile upload functionality so that an administrator can upload a certificate file used for connecting to the wireless network. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "iw_privatePass" is susceptible to this injection. By crafting a packet that contains shell metacharacters, it is possible for an attacker to execute the attack.	2019-06-07	not yet calculated	CVE-2018-10699 MISC BUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. The Moxa AWK 3121 provides ping functionality so that an administrator can execute ICMP calls to check if the network is working correctly. However, the same functionality allows an	2019-06-07	not yet calc	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to execute commands on the device. The POST parameter "srvName" is susceptible to this injection. By crafting a packet that contains shell metacharacters, it is possible for an attacker to execute the attack.		ulated	10697 MISCBUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. The device enables an unencrypted TELNET service by default. This allows an attacker who has been able to gain an MITM position to easily sniff the traffic between the device and the user. Also an attacker can easily connect to the TELNET daemon using the default credentials if they have not been changed by the user.	2019-06-07	not yet calculated	CVE-2018-10698 MISCBUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.19 devices. It provides functionality so that an administrator can change the name of the device. However, the same functionality allows an attacker to execute XSS by injecting an XSS payload. The POST parameter "iw_board_deviceName" is susceptible to this injection.	2019-06-07	not yet calculated	CVE-2018-10700 MISC BUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides functionality so that an administrator can run scripts on the device to troubleshoot any issues. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "iw_filename" is susceptible to buffer overflow. By crafting a packet that contains a string of 162 characters, it is possible for an attacker to execute the attack.	2019-06-07	not yet calculated	CVE-2018-10701 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				UGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides functionality so that an administrator can run scripts on the device to troubleshoot any issues. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "iw_filename" is susceptible to command injection via shell metacharacters.	2019-06-07	not yet calculated	CVE-2018-10702 MISC BUGTRAQ
moxa -- awk-3121	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides functionality so that an administrator can run scripts on the device to troubleshoot any issues. However, the same functionality allows an attacker to execute commands on the	2019-06-07	not yet calc	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device. The POST parameter "iw_serverip" is susceptible to buffer overflow. By crafting a packet that contains a string of 480 characters, it is possible for an attacker to execute the attack.		ulated	10703 MISCBUGTRAQ
multiple_vendors -- multiple_devices	Broadcom firmware before summer 2014 on Nexus 5 BCM4335C0 2012-12-11, Raspberry Pi 3 BCM43438A1 2014-06-02, and unspecifed other devices does not properly restrict LMP commnds and executes certain memory contents upon receiving an LMP command, as demonstrated by executing an HCI command.	2019-06-07	not yet calculated	CVE-2018-19860 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- insight_cloud	NETGEAR Insight Cloud with firmware before Insight 5.6 allows remote authenticated users to achieve command injection.	2019-06-03	not yet calculated	CVE-2019-12591 MISC
nextcloud -- nextcloud	An OS Command Injection has been discovered in the Nextcloud App: Extract prior to version 1.2.0.	2019-06-07	not yet calculated	CVE-2019-5441 MISC
nextcloud -- nextcloud	lib/Controller/ExtractionController.php in the Extract add-on before 1.2.0 for Nextcloud allows Remote Code Execution via shell metacharacters in a RAR filename via ajax/extractRar.php (nameOfFile and directory parameters).	2019-06-05	not yet calcul	CVE-2019-1273

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			ated	9 MISC MISC
nuuo -- network_video_recorder_firmware	NUUO Network Video Recorder Firmware 1.7.x through 3.3.x allows unauthenticated attackers to execute arbitrary commands via shell metacharacters to handle_load_config.php.	2019-05-31	not yet calculated	CVE-2019-9653 MISC MISC MISC
nvidia -- geforce_experience	NVIDIA GeForce Experience versions prior to 3.19 contains a vulnerability in the Web Helper component, in which an attacker with local system access can craft input that may not be properly validated. Such an attack may lead to code execution, denial of service or information disclosure.	2019-05-31	not yet calcul	CVE-2019-56

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			ated	78 CONFIRM
orpak -- siteomat	An insecure communication was found between a user and the Orpak SiteOmat management console for all known versions, due to an invalid SSL certificate. The attack allows for an eavesdropper to capture the communication and decrypt the data.	2019-06-03	not yet calculated	CVE-2017-14852 MISC BID MISC
orpak -- siteomat	A SQL injection vulnerability exists in all Orpak SiteOmat versions prior to 2017-09-25. The vulnerability is in the login page, where the authentication validation process contains an insecure SELECT query. The attack allows for authentication bypass.	2019-06-03	not yet calcul	CVE-2017-14

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			ated	851 BID MISC MISC
orpak -- siteomat	An authentication bypass was found in an unknown area of the SiteOmat source code. All SiteOmat BOS versions are affected, prior to the submission of this exploit. Also, the SiteOmat does not force administrators to switch passwords, leaving SSH and HTTP remote authentication open to public.	2019-06-03	not yet calculated	CVE-2017-14728 MISC BID MISC
orpak -- siteomat	All known versions of the Orpak SiteOmat web management console is vulnerable to multiple instances of Stored Cross-site Scripting due to improper external user-	2019-06	not yet	CVE-20

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	input validation. An attacker with access to the web interface is able to hijack sessions or navigate victims outside of SiteOmat, to a malicious server owned by him.	-03	calculated	17-14850 BID MISC MISC
panasonic -- fpwin_pro	Panasonic FPWIN Pro version 7.3.0.0 and prior allows attacker-created project files to be loaded by an authenticated user triggering incompatible type errors because the resource does not have expected properties. This may lead to remote code execution.	2019-06-07	not yet calculated	CVE-2019-6532 BID MISC
panasonic -- fpwin_pro	Panasonic FPWIN Pro version 7.3.0.0 and prior allows attacker-created project files to be loaded by an authenticated user causing heap-based buffer overflows, which may lead to remote code execution.	2019-06	not yet ca	CVE-2019

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
		-07	lculated	-6530 BIDMISC
papercut -- papercut_mf_and_papercut_ng	An unspecified vulnerability in the application server in PaperCut MF and NG versions 18.3.8 and earlier and versions 19.0.3 and earlier allows remote attackers to execute arbitrary code via an unspecified vector.	2019-06-06	not yet calculated	CVE-2019-12135 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpscriptsmall.com -- api_based_travel_booking	An issue was discovered in PHP Scripts Mall API Based Travel Booking 3.4.7. There is Reflected XSS via the flight-results.php d2 parameter.	2019-06-06	not yet calculated	CVE-2019-7554 MISC MISC
pivotal -- pivotal_ops_manager	The Pivotal Ops Manager, 2.2.x versions prior to 2.2.23, 2.3.x versions prior to 2.3.16, 2.4.x versions prior to 2.4.11, and 2.5.x versions prior to 2.5.3, contain configuration that circumvents refresh token expiration. A remote authenticated user can gain access to a browser session that was supposed to have expired, and access Ops Manager resources.	2019-06-06	not yet calculated	CVE-2019-3790 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pivotal -- spring_data_jpa	This affects Spring Data JPA in versions up to and including 2.1.6, 2.0.14 and 1.11.20. ExampleMatcher using ExampleMatcher.StringMatcher.STARTING, ExampleMatcher.StringMatcher.ENDING or ExampleMatcher.StringMatcher.CONTAINING could return more results than anticipated when a maliciously crafted example value is supplied.	2019-06-03	not yet calculated	CVE-2019-3802 CONFIRM
progress -- sitefinity	Progress Sitefinity 10.1.6536 does not invalidate session cookies upon logouts. It instead tries to overwrite the cookie in the browser, but it remains valid on the server side. This means the cookie can be reused to maintain access to the account, even if the account credentials and permissions are changed.	2019-06-06	not yet calculated	CVE-2019-7215 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
python -- python	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application.	2019-06-07	not yet calculated	CVE-2019-10160 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM C

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ONFIRMMISC
quest -- kace_k1000_appliance	The Quest Kace K1000 Appliance, versions prior to 9.0.270, allows a remote attacker to exploit the misconfigured Cross-Origin Resource Sharing (CORS) mechanism. An unauthenticated, remote attacker could exploit this vulnerability to perform sensitive actions such as adding a new administrator account or changing the appliance?s settings. A malicious internal user could also gain administrator privileges of this appliance and use it to visit a malicious link that exploits this vulnerability. This could cause the application to perform sensitive actions such as adding a new administrator account or changing the appliance?s settings. An unauthenticated, remote attacker could add an administrator-level account or change the appliance's settings.	2019-06-03	not yet calculated	CVE-2018-5406MISCCONFIRMCERT-VN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
quest -- kace_k1000_appliance	The Quest Kace K1000 Appliance, versions prior to 9.0.270, allows an authenticated least privileged user with 'User Console Only' rights to potentially inject arbitrary JavaScript code on the tickets page. Script execution could allow a malicious user of the system to steal session cookies of other users including Administrator and take over their session. This can further be exploited to launch other attacks. The software also does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other user. An authenticated user with 'user console only' rights may inject arbitrary JavaScript, which could result in an attacker taking over a session of others, including an Administrator.	2019-06-03	not yet calculated	CVE-2018-5405 MISC CONFIRM CERT-VN
quest -- kace_k1000_appliance	The Quest Kace K1000 Appliance, versions prior to 9.0.270, allows an authenticated, remote attacker with least privileges ('User Console Only' role) to potentially exploit multiple Blind SQL Injection vulnerabilities to retrieve sensitive information from the database or copy the entire database. An authenticated	2019-06-03	not yet calculated	CVE-2018-5404 C

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote attacker could leverage Blind SQL injections to obtain sensitive data.			ONFIRMCERT-VN
rancher -- rancher	In Rancher 2 through 2.2.3, Project owners can inject additional fluentd configuration to read files or execute arbitrary commands inside the fluentd container.	2019-06-06	not yet calculated	CVE-2019-12303 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rancher -- rancher	In Rancher 1 and 2 through 2.2.3, unprivileged users (if allowed to deploy nodes) can gain admin access to the Rancher management plane because node driver options intentionally allow posting certain data to the cloud. The problem is that a user could choose to post a sensitive file such as /root/.kube/config or /var/lib/rancher/management-state/cred/kubeconfig-system.yaml.	2019-06-06	not yet calculated	CVE-2019-12274 CONFIRM CONFIRM
salesagility -- suitecrm	SuiteCRM 7.8.x before 7.8.30, 7.10.x before 7.10.17, and 7.11.x before 7.11.5 allows SQL Injection (issue 2 of 3).	2019-06-07	not yet calculated	CVE-2019-12600 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
salesagility -- suitecrm	SuiteCRM 7.8.x before 7.8.30, 7.10.x before 7.10.17, and 7.11.x before 7.11.5 allows SQL Injection (issue 3 of 3).	2019-06-07	not yet calculated	CVE-2019-12601 CONFIRM
salesagility -- suitecrm	SuiteCRM 7.10.x before 7.10.17 and 7.11.x before 7.11.5 allows SQL Injection.	2019-06-07	not yet calculated	CVE-2019-12599 CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				FIRM
salesagility -- suitecrm	SuiteCRM 7.8.x before 7.8.30, 7.10.x before 7.10.17, and 7.11.x before 7.11.5 allows SQL Injection (issue 1 of 3).	2019-06-07	not yet calculated	CVE-2019-12598 CONFIRM
samsung -- galaxy_apps	Samsung Galaxy Apps before 4.4.01.7 allows modification of the hostname used for load balancing on installations of applications through a man-in-the-middle attack. An attacker may trick Galaxy Apps into using an arbitrary hostname for which the attacker can provide a valid SSL certificate, and emulate the API of the app store to modify existing apps at installation time. The specific flaw involves an HTTP method to obtain the load-balanced hostname that enforces SSL only after obtaining a hostname from the load	2019-06-07	not yet calculated	CVE-2018-20135 MISCM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	balancer, and a missing app signature validation in the application XML. An attacker can exploit this vulnerability to achieve Remote Code Execution on the device. The Samsung ID is SVE-2018-12071.			ISC
samsung -- galaxy_s9	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Samsung Galaxy S9 prior to 1.4.20.2. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the GameServiceReceiver update mechanism. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7477.	2019-06-03	not yet calculated	CVE-2019-6742 MISC
samsung -- galaxy_s9	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Samsung Galaxy S9 prior to January 2019 Security Update (SMR-JAN-2019 - SVE-2018-13467). User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the ASN.1 parser. When parsing ASN.1 strings, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this	2019-06-03	not yet calculated	CVE-2019-6740 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to execute code in the context of the current process. Was ZDI-CAN-7472.			
samsung -- galaxy_s9	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Samsung Galaxy S9 prior to January 2019 Security Update (SMR-JAN-2019 - SVE-2018-13467). User interaction is required to exploit this vulnerability in that the target must connect to a wireless network. The specific flaw exists within the captive portal. By manipulating HTML, an attacker can force a page redirection. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7476.	2019-06-03	not yet calculated	CVE-2019-6741 MISC
scamera -- security_camera_cz_application	The Security Camera CZ application through 1.6.8 for Android stores potentially sensitive recorded video in external data storage, which is readable by any application.	2019-06-07	not yet calculated	CVE-2019-12763 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sitecore -- experience_platform	Sitecore Experience Platform (XP) prior to 9.1.1 is vulnerable to remote code execution via deserialization, aka TFS # 293863. An authenticated user with necessary permissions is able to remotely execute OS commands by sending a crafted serialized object.	2019-06-06	not yet calculated	CVE-2019-11080 MISC MISC
solarwinds -- serv-u_ftp_server	The local management interface in SolarWinds Serv-U FTP Server 15.1.6.25 has incorrect access controls that permit local users to bypass authentication in the application and execute code in the context of the Windows SYSTEM account, leading to privilege escalation. To exploit this vulnerability, an attacker must have local access the the host running Serv-U, and a Serv-U administrator have an active management console session.	2019-06-07	not yet calculated	CVE-2018-19999 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
soyal -- ar-727h_and_ar-829ev5_devices	On SOYAL AR-727H and AR-829Ev5 devices, all CGI programs allow unauthenticated POST access.	2019-06-06	not yet calculated	CVE-2019-6451 MISC MISC
supra -- smart_cloud_tv	Supra Smart Cloud TV allows remote file inclusion in the openLiveURL function, which allows a local attacker to broadcast fake video without any authentication via a /remote/media_control?action=setUri&uri=URI.	2019-06-07	not yet calculated	CVE-2019-12477 MISC MISC
synaptics -- sound_device_drivers	Incorrect access control in the CxUtilSvc component of the Synaptics Sound Device	2019	not	CV

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	drivers prior to version 2.29 allows a local attacker to increase access privileges to the Windows Registry via an unpublished API.	-06-05	yet calculated	E-2019-9730 CONFIRM MISC MISC
thinstation -- thinstation	Command injection is possible in ThinStation through 6.1.1 via shell metacharacters after the cgi-bin/CdControl.cgi action= substring, or after the cgi-bin/VolControl.cgi OK= substring.	2019-06-07	not yet calculated	CVE-2019-12771 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
thomson_reuters -- desktop	An issue was discovered in Thomson Reuters Desktop Extensions 1.9.0.358. An unauthenticated directory traversal and local file inclusion vulnerability in the ThomsonReuters.Desktop.Service.exe and ThomsonReuters.Desktop.exe allows a remote attacker to list or enumerate sensitive contents of files via a \.. to port 6677. Additionally, this could allow for privilege escalation by dumping the affected machine's SAM and SYSTEM database files, as well as remote code execution.	2019-06-05	not yet calculated	CVE-2019-8385 MISC MISC
tp-link -- tl-wr940n_router	TP-Link TL-WR940N is vulnerable to a stack-based buffer overflow, caused by improper bounds checking by the ipAddrDispose function. By sending specially crafted ICMP echo request packets, a remote authenticated attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges.	2019-06-06	not yet calculated	CVE-2019-6989 MISC
ubiquiti -- edgeos_on_edgerouter_lite_devices	Ubiquiti EdgeOS 1.9.1 on EdgeRouter Lite devices allows remote attackers to execute arbitrary code with admin credentials, because /opt/vyatta/share/vyatta-cfg/templates/system/static-host-mapping/host-name/node.def does not	2019-06-07	not yet calc	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sanitize the 'alias' or 'ips' parameter for shell metacharacters.		ulated	5265 MISC
ubiquiti -- unifi_52_devices	Ubiquiti UniFi 52 devices, when Hotspot mode is used, allow remote attackers to bypass intended restrictions on "free time" Wi-Fi usage by sending a /guest/s/default/ request to obtain a cookie, and then using this cookie in a /guest/s/default/login request with the byfree parameter.	2019-06-07	not yet calculated	CVE-2018-5264 MISC
vmware -- tools	VMware Tools for Windows (10.x before 10.3.10) update addresses an out of bounds read vulnerability in vm3dmp driver which is installed with vmtools in Windows guest machines. A local attacker with non-administrative access to a Windows guest with VMware Tools installed may be able to leak kernel information or create a denial of service attack on the same Windows guest machine.	2019-06-06	not yet calculated	CVE-2019-5522 BID CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM
vmware -- workstation	VMware Workstation (15.x before 15.1.0) contains a use-after-free vulnerability in the Advanced Linux Sound Architecture (ALSA) backend. A malicious user with normal user privileges on the guest machine may exploit this issue in conjunction with other issues to execute code on the Linux host where Workstation is installed.	2019-06-06	not yet calculated	CVE-2019-5525 BID CONFIRM
wordpress -- wordpress	The WP Live Chat Support Pro plugin through 8.0.26 for WordPress contains an arbitrary file upload vulnerability. This results from an incomplete patch for CVE-2018-12426. Arbitrary file upload is achieved by using a non-blacklisted executable file extension in conjunction with a whitelisted file extension, and prepending "magic bytes" to the payload to pass MIME checks. Specifically, an unauthenticated remote user submits a crafted file upload POST request to the REST api remote_upload endpoint. The	2019-06-03	not yet calculated	CVE-2019-11185 MISC M

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	file contains data that will fool the plugin's MIME check into classifying it as an image (which is a whitelisted file extension) and finally a trailing .phtml file extension.			ISCMISC
workday -- workday	CSV Injection (aka Excel Macro Injection or Formula Injection) exists in the export feature in Workday through 32 via a value (provided by a low-privileged user in a contact form field) that is mishandled in a CSV export.	2019-06-06	not yet calculated	CVE-2019-12134 MISC
x-cart -- x-cart	X-Cart V5 is vulnerable to XSS via the CategoryFilter2 parameter.	2019-06-06	not yet calculated	CVE-2019-7220 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xiaomi -- mi6_browser	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Xiaomi Mi6 Browser prior to 10.4.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the WebAssembly.Instance method. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7466.	2019-06-03	not yet calculated	CVE-2019-6743 MISC
xiaomi -- mi_5s_plus_devices	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch.	2019-06-06	not yet calculated	CVE-2019-12762 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xiaomi -- redmi_note_5_pro_devices_and_redmi_android_phones	Xiaomi Stock Browser 10.2.4.g on Xiaomi Redmi Note 5 Pro devices and other Redmi Android phones allows content provider injection. In other words, a third-party application can read the user's cleartext browser history via an app.provider.query content://com.android.browser.searchhistory/searchhistory request.	2019-06-07	not yet calculated	CVE-2018-20523 MISC MISC