Vulnerability Summary for the Week of June 29, 2020

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
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9566 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9564 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9562 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful	2020-06-26	9.3	CVE-2020-9569

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation could lead to arbitrary code execution .			CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9568 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9565 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9567 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9563 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9559 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9560 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9556 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9555 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9554 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9561 CONFIRM
adobe -- character_animator	Adobe Character Animator versions 3.2 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9586 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9589 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful	2020-06-26	9.3	CVE-2020-9590

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation could lead to arbitrary code execution.			CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9620 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9621 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9573 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9574 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9572 CONFIRM
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	9.3	CVE-2020-9571 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-06-26	9.3	CVE-2020-9570 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9585 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9576 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9582 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9583 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9580 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	10	CVE-2020-9631 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9578 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a business logic error vulnerability. Successful exploitation could lead to privilege escalation.	2020-06-26	7.5	CVE-2020-9630 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	10	CVE-2020-9632 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-06-26	7.5	CVE-2020-9579 CONFIRM
draytek -- multiple_devices	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is	2020-06-30	7.5	CVE-2020-15415 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	used, a different issue than CVE-2020-14472.			
f5 -- big-ip	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.	2020-07-01	10	CVE-2020-5902 MISC
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. The web login functionality allows an attacker to bypass authentication and gain client privileges via SQL injection in central/executar_login.php.	2020-06-29	7.5	CVE-2020-14068 MISC MISC
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. It allows command execution as root via shell metacharacters to /auth admin scripts.	2020-06-29	10	CVE-2020-14072 MISC MISC
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. There is authentication bypass in the web login functionality because guessable credentials to admin/executar_login.php result in admin access.	2020-06-29	10	CVE-2020-14070 MISC MISC
opensis -- opensis	openSIS through 7.4 allows SQL Injection.	2020-07-01	7.5	CVE-2020-13381 MISC MISC
opensis -- opensis	openSIS before 7.4 allows SQL Injection.	2020-07-01	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				13380 CONFIRM MISC
prestashop -- prestashop	In PrestaShop from version 1.6.0.1 and before version 1.7.6.6, the dashboard allows rewriting all configuration variables. The problem is fixed in 1.7.6.6	2020-07-02	7.5	CVE-2020-15082 MISC CONFIRM
prestashop -- prestashop	In PrestaShop from version 1.5.0.0 and before version 1.7.7.6, the authentication system is malformed and an attacker is able to forge requests and execute admin commands. The problem is fixed in 1.7.7.6.	2020-07-02	10	CVE-2020-4074 MISC CONFIRM
sqlite -- sqlite	In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.	2020-06-27	7.5	CVE-2020-15358 MISC MISC MISC
stash -- stash	Stash 1.0.3 allows SQL Injection via the downloadmp3.php download parameter.	2020-06-26	7.5	CVE-2020-15311 MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the axiros password for the root account.	2020-06-29	7.5	CVE-2020-15320 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a world-readable axess/opt/axXMPPHandler/config/xmpp	2020-06-29	7.5	CVE-2020-15324

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	_config.py file that stores hardcoded credentials.			MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- after_effects	Adobe After Effects versions 17.0.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-3809 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9553 CONFIRM
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9557 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- bridge	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9558 CONFIRM
adobe -- coldfusion	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an improper access control vulnerability. Successful exploitation could lead to system file structure disclosure.	2020-06-26	4.3	CVE-2020-3796 CONFIRM
adobe -- coldfusion	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an insufficient input validation vulnerability. Successful exploitation could lead to application-level denial-of-service (dos).	2020-06-26	4.3	CVE-2020-3767 CONFIRM
adobe -- coldfusion	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have a dll search-order hijacking vulnerability. Successful exploitation could lead to privilege escalation.	2020-06-26	4.4	CVE-2020-3768 CONFIRM
adobe -- digital_editions	Adobe Digital Editions versions 4.5.11.187212 and below have a file	2020-06-26	4.3	CVE-2020-3798

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	enumeration (host or local network) vulnerability. Successful exploitation could lead to information disclosure.			CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	5	CVE-2020-9627 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9622 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9624 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read	2020-06-26	5	CVE-2020-9628 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability. Successful exploitation could lead to information disclosure.			
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9626 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	5	CVE-2020-9625 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9629 CONFIRM
adobe -- dng_software_development_kit	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation	2020-06-26	5	CVE-2020-9623 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could lead to information disclosure.			
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to unauthorized access to admin panel.	2020-06-26	5	CVE-2020-9591 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an observable timing discrepancy vulnerability. Successful exploitation could lead to signature verification bypass.	2020-06-26	6.5	CVE-2020-9588 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2020-06-26	4.3	CVE-2020-9577 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2020-06-26	4.3	CVE-2020-9581 CONFIRM
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an authorization bypass vulnerability. Successful exploitation could lead to potentially unauthorized product discounts.	2020-06-26	5	CVE-2020-9587 CONFIRM
adobe -- premiere_pro	Adobe Premiere Pro versions 14.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9616 CONFIRM
adobe -- premiere_rush	Adobe Premiere Rush versions 1.5.8 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2020-06-26	4.3	CVE-2020-9617 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- tomcat	A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.	2020-06-26	5	CVE-2020-11996 MLIST CONFIRM MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST
cybozu -- garoon	Path traversal vulnerability in Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to obtain unintended information via unspecified vectors.	2020-06-30	4	CVE-2020-5581 MISC MISC
cybozu -- garoon	Path traversal vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to obtain unintended information via unspecified vectors.	2020-06-30	4	CVE-2020-5588 MISC MISC
docker -- docker_desktop	com.docker.vmnetd in Docker Desktop 2.3.0.3 allows privilege escalation because of a	2020-06-27	4.6	CVE-2020-15360 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lack of client verification.			
ibm -- api_connect	IBM API Connect V2018.4.1.0 through 2018.4.1.11 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 181324.	2020-06-29	5	CVE-2020-4452 XF CONFIRM
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.1.1 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 170961.	2020-06-26	6.5	CVE-2019-4650 XF CONFIRM
ibm -- security_identity_manager_virtual_appliance	IBM Security Identity Manager Virtual Appliance 7.0.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 172015.	2020-07-01	4	CVE-2019-4705 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_identity_manager_virtual_appliance	IBM Security Identity Manager Virtual Appliance 7.0.2 writes information to log files which can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. IBM X-Force ID: 172016.	2020-07-01	4	CVE-2019-4706 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow an attacker to obtain sensitive information due to insecure communications being used between the application and server. IBM X-Force ID: 183935.	2020-06-26	4.3	CVE-2020-4565 XF CONFIRM
jiangmin -- jiangmin_antivirus	In Jiangmin Antivirus 16.0.13.129, the driver file (KVFG.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x220440.	2020-06-26	4.9	CVE-2020-14955 MISC
mattermost -- mattermost_mobile_app	An issue was discovered in Mattermost Mobile Apps before 1.31.2 on iOS. Unintended third-party servers could sometimes obtain	2020-06-26	5	CVE-2020-13891 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authorization tokens, aka MMSA-2020-0022.			
mediaarea -- mediainfo	In MediaInfoLib in MediaArea MediaInfo 20.03, there is a stack-based buffer over-read in Streams_Fill_PerStream in Multiple/File_MpegPs.cpp (aka an off-by-one during MpegPs parsing).	2020-06-30	6.8	CVE-2020-15395 MISC MISC
mk-auth -- mk-auth	IBM Security Identity Manager Virtual Appliance 7.0.2 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 172014.	2020-07-01	4.3	CVE-2019-4704 XF CONFIRM
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. XSS vulnerabilities in admin and client scripts allow	2020-06-29	4.3	CVE-2020-14071 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	an attacker to execute arbitrary JavaScript code.			
mk-auth -- mk-auth	An issue was discovered in MK-AUTH 19.01. There are SQL injection issues in mkt/ PHP scripts, as demonstrated by arp.php, dhcp.php, hotspot.php, ip.php, pgaviso.php, pgcorte.php, pppoe.php, queues.php, and wifi.php.	2020-06-29	4.6	CVE-2020-14069 MISC MISC
nedi_consulting -- nedi	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Other-Converter.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the txt GET parameter.	2020-06-26	4.3	CVE-2020-15016 MISC
nedi_consulting -- nedi	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Devices-Config.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary	2020-06-26	4.3	CVE-2020-15017 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	JavaScript in the sta GET parameter.			
opensis -- opensis	openSIS through 7.4 allows Directory Traversal.	2020-07-01	5	CVE-2020-13383 MISC MISC
opensis -- opensis	openSIS through 7.4 has Incorrect Access Control.	2020-07-01	6.4	CVE-2020-13382 MISC MISC
prestashop -- prestashop	In PrestaShop from version 1.7.0.0 and before version 1.7.6.6, if a target sends a corrupted file, it leads to a reflected XSS. The problem is fixed in 1.7.6.6	2020-07-02	4.3	CVE-2020-15083 MISC CONFIRM
prestashop -- prestashop	In PrestaShop from version 1.5.0.0 and before 1.7.6.6, there is information exposure in the upload directory. The problem is fixed in version 1.7.6.6. A possible workaround is to add an empty index.php file in the upload directory.	2020-07-02	5	CVE-2020-15081 MISC CONFIRM
wordpress -- wordpress	The Nexos theme through 1.7 for WordPress allows top-map/?search_location= reflected XSS.	2020-06-28	4.3	CVE-2020-15364 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Nexos theme through 1.7 for WordPress allows side-map/?search_order= SQL Injection.	2020-06-28	5	CVE-2020-15363 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account within the /opt/mysql chroot directory tree.	2020-06-29	4.3	CVE-2020-15319 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account.	2020-06-29	4.3	CVE-2020-15314 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded ECDSA SSH key for the root account.	2020-06-29	4.3	CVE-2020-15313 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account.	2020-06-29	4.3	CVE-2020-15312 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- magento	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2020-06-26	3.5	CVE-2020-9584 CONFIRM
adobe -- magento	Form Builder 2.1.0 for Magento has multiple XSS issues that can be exploited against Magento 2 admin accounts via the Current_url or email field, or the User-Agent HTTP header.	2020-06-29	3.5	CVE-2020-13423 MISC MISC MISC
atlassian -- jira_server_and_data_center	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a vnd.wap.xhtml+xml content type.	2020-07-01	3.5	CVE-2020-4024 MISC
avast -- avast_antivirus	An elevation of privilege vulnerability exists in Avast Free Antivirus and AVG AntiVirus Free before 20.4 due to improperly handling hard links. The vulnerability allows local users to take control of arbitrary files.	2020-06-29	2.1	CVE-2020-13657 CONFIRM CONFIRM
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors.	2020-06-30	3.5	CVE-2020-5585 MISC MISC
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.10.3 to 5.0.1	2020-06-30	3.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows attacker with administrator rights to inject an arbitrary script via unspecified vectors.			5586 MISC MISC
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.0.10 and 7.6.1.1 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: 175121.	2020-06-26	3.5	CVE-2020-4223 XF CONFIRM
ibm -- security_identity_manager_virtual_appliance	IBM Security Identity Manager Virtual Appliance 7.0.2 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 171512.	2020-07-01	2.1	CVE-2019-4676 XF CONFIRM
linux -- linux_kernel	In the Linux kernel through 5.7.6, usbtest_disconnect in drivers/usb/misc/usbtest.c has a memory leak, aka CID-28ebeb8db770.	2020-06-29	2.1	CVE-2020-15393 MISC MISC
openexr -- openexr	An issue was discovered in OpenEXR before 2.5.2. An invalid tiled input file could cause invalid memory access in TiledInputFile::TiledInputFile() in IlmImf/ImfTiledInputFile.cpp, as demonstrated by a NULL pointer dereference.	2020-06-26	2.1	CVE-2020-15304 MISC MISC MISC MISC
openexr -- openexr	An issue was discovered in OpenEXR before 2.5.2. Invalid input could cause a use-after-free in DeepScanLineInputFile::DeepScan	2020-06-26	2.1	CVE-2020-15305 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	LineInputFile() in IlmImf/ImfDeepScanLineInputFile.cpp.			MISC MISC MISC
openexr -- openexr	An issue was discovered in OpenEXR before v2.5.2. Invalid chunkCount attributes could cause a heap buffer overflow in getChunkOffsetTableSize() in IlmImf/ImfMisc.cpp.	2020-06-26	2.1	CVE-2020-15306 MISC MISC MISC MISC
prestashop -- prestashop	In PrestaShop from version 1.5.3.0 and before version 1.7.7.6, there is a stored XSS when using the name of a quick access item. The problem is fixed in 1.7.7.6.	2020-07-02	3.5	CVE-2020-11074 MISC CONFIRM

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mitsubishi_electric -- multiple_fa_engineering_software_products	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver.	2020-06-30	not yet calculated	CVE-2020-5603 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors.			
activision -- call_of_duty_modern_warfare_2	An issue was discovered in Activision Infinity Ward Call of Duty Modern Warfare 2 through 2019-12-11. PartyHost_HandleJoinPartyRequest has a buffer overflow vulnerability and can be exploited by using a crafted joinParty packet. This can be utilized to conduct arbitrary code execution on a victim's machine.	2020-06-30	not yet calculated	CVE-2019-20893 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- guacamole	Apache Guacamole 1.1.0 and older may mishandle pointers involved inprocessing data received via RDP static virtual channels. If a userconnects to a malicious or compromised RDP server, a series ofspecially-crafted PDUs could result in memory corruption, possiblyallowing arbitrary code to be executed with the privileges of therunning guacd process.	2020-07-02	not yet calculated	CVE-2020-9498 MLIST MISC
apache -- guacamole	Apache Guacamole 1.1.0 and older do not properly validate datareceived from RDP servers via static virtual channels. If a userconnects to a malicious or compromised RDP server, specially-craftedPDUs could result in disclosure of information within the memory ofthe guacd process handling the connection.	2020-07-02	not yet calculated	CVE-2020-9497 MLIST MLIST MLIST MISC
asrock -- rgb_driver	AsrDrv103.sys in the ASRock RGB Driver does not properly restrict access from user space, as demonstrated by triggering a triple fault via a request to zero CR3.	2020-06-29	not yet calculated	CVE-2020-15368 MISC
atlassian -- confluence_server_and_data_center	Atlassian Confluence Server and Data Center before version 7.5.1 allowed remote attackers with system administration permissions to bypass velocity template injection mitigations via an injection vulnerability in custom user macros.	2020-07-01	not yet calculated	CVE-2020-4027 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- jira	The /plugins/servlet/gadgets/makeRequest resource in Jira before version 8.7.0 allows remote attackers to access the content of internal network resources via a Server Side Request Forgery (SSRF) vulnerability due to a logic bug in the JiraWhitelist class.	2020-07-01	not yet calculated	CVE-2019-20408 MISC
atlassian -- jira_desk_server_and_data_center	The /servicedesk/customer/portals resource in Jira Service Desk Server and Data Center before version 4.10.0 allows remote attackers with project administrator privileges to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by uploading a html file.	2020-07-01	not yet calculated	CVE-2020-14166 MISC
atlassian -- jira_server_and_data_center	The /rest/project-templates/1.0/createshared resource in Atlassian Jira Server and Data Center before version 8.5.5, from 8.6.0 before 8.7.2, and from 8.8.0 before 8.8.1 allows remote attackers to enumerate project names via an improper authorization vulnerability.	2020-07-01	not yet calculated	CVE-2020-4029 MISC
atlassian -- jira_server_and_data_center	The file upload feature in Atlassian Jira Server and Data Center in affected versions allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability. The affected versions are before version	2020-07-03	not yet calculated	CVE-2020-14173 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8.5.4, from version 8.6.0 before 8.6.2, and from version 8.7.0 before 8.7.1.			
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability on the UserPickerBrowser.jspa page. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	2020-06-29	not yet calculated	CVE-2019-20413 N/A
atlassian -- jira_server_and_data_center	The attachment download resource in Atlassian Jira Server and Data Center The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a rdf content type.	2020-07-01	not yet calculated	CVE-2020-4025 MISC
atlassian -- jira_server_and_data_center	The quick search component in Atlassian Jira Server and Data Center before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability	2020-07-01	not yet calculated	CVE-2020-14169 MISC
atlassian -- jira_server_and_data_center	The MessageBundleResource resource in Jira Server and Data Center before version 7.13.4, from 8.5.0 before 8.5.5, from 8.8.0 before 8.8.2, and from	2020-07-01	not yet calculated	CVE-2020-14167 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8.9.0 before 8.9.1 allows remote attackers to impact the application's availability via an Denial of Service (DoS) vulnerability.			
atlassian -- jira_server_and_data_center	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a mixed multipart content type.	2020-07-01	not yet calculated	CVE-2020-4022 MISC
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to achieve template injection via the Web Resources Manager. The affected versions are before version 8.8.1.	2020-07-03	not yet calculated	CVE-2020-14172 MISC
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate internal services via an Information Disclosure vulnerability. The vulnerability is only exploitable if WebSudo is disabled in Jira. The affected versions are before version 8.4.2.	2020-07-02	not yet calculated	CVE-2019-20417 MISC
atlassian -- jira_server_and_data_center	The email client in Jira Server and Data Center before version 7.13.16, from 8.5.0 before 8.5.7, from 8.8.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows	2020-07-01	not yet calculated	CVE-2020-14168 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote attackers to access outgoing emails between a Jira instance and the SMTP server via man-in-the-middle (MITM) vulnerability.			
atlassian -- jira_server_and_data_center	The Convert Sub-Task to Issue page in affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate the following information via an Improper Authentication vulnerability: Workflow names; Project Key, if it is part of the workflow name; Issue Keys; Issue Types; Status Types. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	2020-06-29	not yet calculated	CVE-2019-20412 MISC
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the project configuration feature. The affected versions are before version 8.3.0.	2020-06-30	not yet calculated	CVE-2019-20416 N/A
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to execute arbitrary code via a DLL hijacking vulnerability in Tomcat. The affected versions are before version 8.5.5, and from version 8.6.0 before 8.7.2.	2020-07-03	not yet calculated	CVE-2019-20419 MISC
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center	2020-07-03	not yet	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allow remote attackers to prevent users from accessing the instance via an Application Denial of Service vulnerability in the /rendering/wiki endpoint. The affected versions are before version 8.8.0.		calculated	20418 N/A
atlassian -- jira_server_and_data_center	Atlassian Jira Server and Data Center in affected versions allows remote attackers to modify logging and profiling settings via a cross-site request forgery (CSRF) vulnerability. The affected versions are before version 7.13.3, and from version 8.0.0 before 8.1.0.	2020-06-30	not yet calculated	CVE-2019-20415 MISC
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in Issue Navigator Basic Search. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	2020-06-29	not yet calculated	CVE-2019-20414 MISC
atlassian -- jira_server_and_data_center	The WYSIWYG editor resource in Jira Server and Data Center before version 8.8.2 allows remote attackers to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by pasting javascript code into the editor field.	2020-07-01	not yet calculated	CVE-2020-14164 MISC
atlassian -- jira_server_and_data_center	The UniversalAvatarResource.getAvatars resource in Jira Server and	2020-07-01	not yet	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Data Center before version 8.9.0 allows remote attackers to obtain information about custom project avatars names via an Improper authorization vulnerability.		calculated	14165 MISC
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify Wallboard settings via a Cross-site request forgery (CSRF) vulnerability. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	2020-06-29	not yet calculated	CVE-2019-20411 MISC
atlassian -- jira_server_and_data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to view sensitive information via an Information Disclosure vulnerability in the comment restriction feature. The affected versions are before version 7.6.17, from version 7.7.0 before 7.13.9, and from version 8.0.0 before 8.4.2.	2020-06-29	not yet calculated	CVE-2019-20410 MISC
baxter -- exactamix_em2400_and_em1200_devices	Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13 and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 does not restrict non administrative users from gaining access to the operating system and editing the application startup script. Successful exploitation of this vulnerability may allow an attacker to alter the startup script as the limited-access user.	2020-06-29	not yet calculated	CVE-2020-12020 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
baxter -- exactamix_em2400_and_em1200_devices	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The PrismaFlex device contains a hard-coded service password that provides access to biomedical information, device settings, calibration settings, and network configuration. This could allow an attacker to modify device settings and calibration.	2020-06-29	not yet calculated	CVE-2020-12035 MISC
baxter -- exactamix_em2400_and_em1200_devices	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems store device data with sensitive information in an unencrypted database. This could allow an attacker with network access to view or modify sensitive data including PHI.	2020-06-29	not yet calculated	CVE-2020-12032 MISC
baxter -- exactamix_em2400_and_em1200_devices	Baxter ExactaMix EM 2400 versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 does not restrict access to the USB interface from an unauthorized user with physical access. Successful exploitation of this vulnerability may allow an attacker with physical access to the system the ability to load an unauthorized payload or unauthorized access to the hard drive by booting a live USB OS. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.	2020-06-29	not yet calculated	CVE-2020-12024 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
baxter -- exactamix_em_2400_and_em1200_devices	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems use cleartext messages to communicate order information with an order entry system. This could allow an attacker with network access to view sensitive data including PHI.	2020-06-29	not yet calculated	CVE-2020-12008 MISC
baxter -- multiple_exactamix_devices	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13, and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 have hard-coded administrative account credentials for the ExactaMix application. Successful exploitation of this vulnerability may allow an attacker with physical access to gain unauthorized access to view/update system configuration or data. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.	2020-06-29	not yet calculated	CVE-2020-12012 MISC
baxter -- multiple_exactamix_devices	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5	2020-06-29	not yet calculated	CVE-2020-12016 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	have hard-coded administrative account credentials for the ExactaMix operating system. Successful exploitation of this vulnerability may allow an attacker who has gained unauthorized access to system resources, including access to execute software or to view/update files, directories, or system configuration. This could allow an attacker with network access to view sensitive data including PHI.			
baxter -- multiple_sigma_spectrum_with_wireless_battery	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when used in conjunction with a Baxter Spectrum v8.x (model 35700BAX2), operates a Telnet service on Port 1023 with hard-coded credentials.	2020-06-29	not yet calculated	CVE-2020-12045 MISC
baxter -- multiple_sigma_spectrum_with_wireless_battery	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) telnet Command-Line Interface, grants access to sensitive data stored on the WBM that permits temporary configuration changes to network settings of the WBM, and allows the WBM to be rebooted. Temporary configuration changes to network settings are removed upon reboot.	2020-06-29	not yet calculated	CVE-2020-12041 MISC
baxter -- multiple_sigma_spectrum_with_wireless_battery	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when configured for wireless networking the FTP	2020-06-29	not yet calculated	CVE-2020-12043 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	service operating on the WBM remains operational until the WBM is rebooted.			
baxter -- multiple_sigma_spectrum_with_wireless_battery	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24), when used with a Baxter Spectrum v8.x (model 35700BAX2) in a factory-default wireless configuration enables an FTP service with hard-coded credentials.	2020-06-29	not yet calculated	CVE-2020-12047 MISC
baxter -- phoenix_hemodialysis_delivery_system	Phoenix Hemodialysis Delivery System SW 3.36 and 3.40, The Phoenix Hemodialysis device does not support data-in-transit encryption (e.g., TLS/SSL) when transmitting treatment and prescription data on the network between the Phoenix system and the Exalis dialysis data management tool. An attacker with access to the network could observe sensitive treatment and prescription data sent between the Phoenix system and the Exalis tool.	2020-06-29	not yet calculated	CVE-2020-12048 MISC
baxter -- prismaflex_devices	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device.	2020-06-29	not yet calculated	CVE-2020-12036 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
baxter -- prismaflex_devices	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device.	2020-06-29	not yet calculated	CVE-2020-12037 MISC
baxter -- sigma_spectrum_infusion_pumps_35700bax_and_35700bax2	Baxter Sigma Spectrum Infusion Pumps Sigma Spectrum Infusion System v's6.x model 35700BAX & Baxter Spectrum Infusion System v's8.x model 35700BAX2 contain hardcoded passwords when physically entered on the keypad provide access to biomedical menus including device settings, view calibration values, network configuration of Sigma Spectrum WBM if installed.	2020-06-29	not yet calculated	CVE-2020-12039 MISC
baxter -- sigma_spectrum_infusion_pumps_35700bax_and_35700bax2	Sigma Spectrum Infusion System v's6.x (model 35700BAX) and Baxter Spectrum Infusion System Version(s) 8.x (model 35700BAX2) at the application layer uses an unauthenticated clear-text communication channel to send and receive system status and operational data. This could allow an attacker that has circumvented network security measures to view sensitive non-private data or to perform a man-in-the-middle attack.	2020-06-29	not yet calculated	CVE-2020-12040 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bcrypt -- bcrypt	Data is truncated wrong when its length is greater than 255 bytes.	2020-07-01	not yet calculated	CVE-2020-7689 MISC MISC MISC MISC
best_it_world -- wrb303n_devices	iBall WRB303N devices allow CSRF attacks, as demonstrated by enabling remote management, enabling DHCP, or modifying the subnet range for IP addresses.	2020-06-29	not yet calculated	CVE-2020-15043 MISC MISC
biotronik -- cardiomessengerii	BIOTRONIK CardioMessenger II, The affected products transmit credentials in clear-text prior to switching to an encrypted communication channel. An attacker can disclose the product's client credentials for connecting to the BIOTRONIK Remote Communication infrastructure.	2020-06-29	not yet calculated	CVE-2019-18248 MISC
biotronik -- cardiomessengerii	BIOTRONIK CardioMessenger II, The affected products allow credential reuse for multiple authentication purposes. An attacker with adjacent access to the CardioMessenger can disclose its credentials used for connecting to the BIOTRONIK Remote Communication infrastructure.	2020-06-29	not yet calculated	CVE-2019-18252 MISC
biotronik -- cardiomessengerii	BIOTRONIK CardioMessenger II, The affected products do not encrypt sensitive information while at rest. An attacker with physical access to the	2020-06-29	not yet calculated	CVE-2019-18254 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CardioMessenger can disclose medical measurement data and the serial number from the implanted cardiac device the CardioMessenger is paired with.			
biotronik -- cardiomessengerii	BIOTRONIK CardioMessenger II, The affected products use individual per-device credentials that are stored in a recoverable format. An attacker with physical access to the CardioMessenger can use these credentials for network authentication and decryption of local data in transit.	2020-06-29	not yet calculated	CVE-2019-18256 MISC
biotronik -- cardiomessengerii_	BIOTRONIK CardioMessenger II, The affected products do not properly enforce mutual authentication with the BIOTRONIK Remote Communication infrastructure.	2020-06-29	not yet calculated	CVE-2019-18246 MISC
broadcom -- brocade_network_advisor	A vulnerability in Brocade Network Advisor Version Before 14.3.1 could allow an unauthenticated, remote attacker to log in to the JBoss Administration interface of an affected system using an undocumented user credentials and install additional JEE applications.	2020-06-29	not yet calculated	CVE-2018-6446 MISC
cabsoftware -- reportexpress_proplus	Reportexpress ProPlus contains a vulnerability that could allow an arbitrary code execution by inserted VBscript into the configure file(rxp).	2020-06-29	not yet calculated	CVE-2019-19160 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cake_software_foundation -- cakephp	CakePHP before 4.0.6 mishandles CSRF token generation. This might be remotely exploitable in conjunction with XSS.	2020-06-30	not yet calculated	CVE-2020-15400 MISC
cellebrite -- ufed	The Cellebrite UFED physical device 5.0 through 7.5.0.845 relies on key material hardcoded within both the executable code supporting the decryption process, and within the encrypted files themselves by using a key enveloping technique. The recovered key material is the same for every device running the same version of the software, and does not appear to be changed with each new build. It is possible to reconstruct the decryption process using the hardcoded key material and obtain easy access to otherwise protected data.	2020-06-30	not yet calculated	CVE-2020-14474 MISC MISC MISC
cisco -- digital_network_architecture_center	A vulnerability in Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to insecure storage of certain unencrypted credentials on an affected device. An attacker could exploit this vulnerability by viewing the network device configuration and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.	2020-07-02	not yet calculated	CVE-2020-3391 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- identity_services_engine	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input that is processed by the web-based management interface. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need valid administrative credentials.	2020-07-02	not yet calculated	CVE-2020-3340 CISCO
cisco -- multiple_products	A vulnerability in the web-based management interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected	2020-07-02	not yet calculated	CVE-2020-3282 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	software. 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 affected interface or access sensitive browser-based information.			
cisco -- small_business_smart_and_managed_switches	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user.	2020-07-02	not yet calculated	CVE-2020-3297 CISCO
cisco -- unified_customer_voice_portal	A vulnerability in the Java Remote Method Invocation (RMI) interface of Cisco Unified Customer Voice Portal (CVP)	2020-07-02	not yet calculated	CVE-2020-3402

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because certain RMI listeners are not properly authenticated. An attacker could exploit this vulnerability by sending a crafted request to the affected listener. A successful exploit could allow the attacker to access sensitive information on an affected device.			CISCO
commax -- cdp_1020mb_wallpad	A Vulnerability in the firmware of COMMAX WallPad(CDP-1020MB) allow an unauthenticated adjacent attacker to execute arbitrary code, because of a using the old version of MySQL.	2020-06-30	not yet calculated	CVE-2019-19163 MISC MISC
containous -- traefik	Traefik 2.x, in certain configurations, allows HTTPS sessions to proceed without mutual TLS verification in a situation where ERR_BAD_SSL_CLIENT_AUTH_CERT should have occurred.	2020-07-02	not yet calculated	CVE-2019-20894 MISC
coturn -- coturn	In coturn before version 4.5.1.3, there is an issue whereby STUN/TURN response buffer is not initialized properly. There is a leak of information between different client connections. One client (an attacker) could use their connection to intelligently query coturn to get interesting bytes in the padding bytes from	2020-06-29	not yet calculated	CVE-2020-4067 MISC MISC CONFIRM MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the connection of another client. This has been fixed in 4.5.1.3.			DEBIAN
cybozu -- garoon	Cybozu Garoon 4.0.0 to 5.0.1 allow remote authenticated attackers to obtain unintended information via unspecified vectors.	2020-06-30	not yet calculated	CVE-2020-5587 MISC MISC
cybozu -- garoon	Cybozu Garoon 4.0.0 to 5.0.1 allow remote attackers to obtain unintended information via unspecified vectors.	2020-06-30	not yet calculated	CVE-2020-5584 MISC MISC
cybozu -- garoon	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to obtain unauthorized Multi-Report's data via unspecified vectors.	2020-06-30	not yet calculated	CVE-2020-5583 MISC MISC
cybozu -- garoon	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to alter the data for the file attached to Report via unspecified vectors.	2020-06-30	not yet calculated	CVE-2020-5582 MISC MISC
cybozu -- garoon	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to view and/or alter Single sign-on settings via unspecified vectors.	2020-06-30	not yet calculated	CVE-2020-5580 MISC MISC
delta_electronics -- delta_industrial_automation_dopsoft	Delta Industrial Automation DOPSoft, Version 4.00.08.15 and prior. Opening a specially crafted project file may overflow	2020-06-30	not yet calculated	CVE-2020-14482 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the heap, which may allow remote code execution, disclosure/modification of information, or cause the application to crash.			
donjon -- ledger_live	Ledger Live before 2.7.0 does not handle Bitcoin's Replace-By-Fee (RBF). It increases the user's balance with the value of an unconfirmed transaction as soon as it is received (before the transaction is confirmed) and does not decrease the balance when it is canceled. As a result, users are exposed to basic double spending attacks, amplified double spending attacks, and DoS attacks without user consent.	2020-07-02	not yet calculated	CVE-2020-12119 CONFIRM
envoy -- envoy	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may exhaust file descriptors and/or memory when accepting too many connections.	2020-07-01	not yet calculated	CVE-2020-8663 CONFIRM MISC
envoy_proxy -- envoy	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may consume excessive amounts of memory when processing HTTP/1.1 headers with long field names or requests with long URLs.	2020-07-01	not yet calculated	CVE-2020-12605 CONFIRM MISC
envoy_proxy -- envoy	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may consume excessive amounts of memory when proxying HTTP/2 requests or responses with many small (i.e. 1 byte) data frames.	2020-07-01	not yet calculated	CVE-2020-12603 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
envoy_proxy -- envoy	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier is susceptible to increased memory usage in the case where an HTTP/2 client requests a large payload but does not send enough window updates to consume the entire stream and does not reset the stream.	2020-07-01	not yet calculated	CVE-2020-12604 MISC CONFIRM
express-jwt -- express-jwt	In express-jwt (NPM package) up and including version 5.3.3, the algorithms entry to be specified in the configuration is not being enforced. When algorithms is not specified in the configuration, with the combination of jwks-rsa, it may lead to authorization bypass. You are affected by this vulnerability if all of the following conditions apply: - You are using express-jwt - You do not have **algorithms** configured in your express-jwt configuration. - You are using libraries such as jwks-rsa as the **secret**. You can fix this by specifying **algorithms** in the express-jwt configuration. See linked GHSA for example. This is also fixed in version 6.0.0.	2020-06-30	not yet calculated	CVE-2020-15084 MISC CONFIRM
f5 -- big-ip	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page.	2020-07-01	not yet calculated	CVE-2020-5904 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip	In versions bundled with BIG-IP APM 12.1.0-12.1.5 and 11.6.1-11.6.5.2, Edge Client for Linux exposes full session ID in the local log files.	2020-07-01	not yet calculated	CVE-2020-5908 MISC
f5 -- big-ip	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display.	2020-07-01	not yet calculated	CVE-2020-5905 MISC
f5 -- big-ip	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility.	2020-07-01	not yet calculated	CVE-2020-5903 MISC
f5 -- big-ip	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality.	2020-07-01	not yet calculated	CVE-2020-5907 MISC
f5 -- big-ip	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP.	2020-07-01	not yet calculated	CVE-2020-5906 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
factorfx -- ocs_inventory	OCS Inventory NG 2.7 allows Remote Command Execution via shell metacharacters to require/commandLine/CommandLine.php because mib_file in plugins/main_sections/ms_config/ms_snmp_config.php is mishandled in get_mib_oid.	2020-06-30	not yet calculated	CVE-2020-14947 MISC MISC MISC MISC
ffjpeg -- ffjpeg	ffjpeg through 2020-02-24 has a heap-based buffer overflow in jfif_decode in jfif.c.	2020-07-01	not yet calculated	CVE-2020-15470 MISC
github -- github	The table extension in GitHub Flavored Markdown before version 0.29.0.gfm.1 takes O(n * n) time to parse certain inputs. An attacker could craft a markdown table which would take an unreasonably long time to process, causing a denial of service. This issue does not affect the upstream cmark project. The issue has been fixed in version 0.29.0.gfm.1.	2020-07-01	not yet calculated	CVE-2020-5238 MISC CONFIRM
hcl -- domino	"A vulnerability in the TLS protocol implementation of the Domino server could allow an unauthenticated, remote attacker to access sensitive information, aka a Return of Bleichenbacher's Oracle Threat (ROBOT) attack. An attacker could iteratively query a server running a vulnerable TLS stack implementation to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions."	2020-07-01	not yet calculated	CVE-2017-1712 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hcl -- inotes	"HCL iNotes is susceptible to a Cross-Site Scripting (XSS) Vulnerability. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials."	2020-07-01	not yet calculated	CVE-2017-1659 MISC
hcl -- notes	HCL Notes is vulnerable to an information leakage vulnerability through its support for the 'mailto' protocol. This vulnerability could result in files from the user's filesystem or connected network filesystems being leaked to a third party. All versions of HCL Notes 9, 10 and 11 are affected.	2020-06-26	not yet calculated	CVE-2020-4089 CONFIRM
human_talk -- daview_indy_and_dava+_and_daoffice_softwares	A vulnerability in the JPEG image parsing module in DaView Indy, DaVa+, DaOffice softwares could allow an unauthenticated, remote attacker to cause an arbitrary code execution on an affected device.nThe vulnerability is due to a stack overflow read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device.	2020-06-30	not yet calculated	CVE-2020-7816 CONFIRM
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 are 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	2020-06-29	not yet calculated	CVE-2020-4557 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to credentials disclosure within a trusted session. IBM X-Force ID: 183611.			
ibm -- db2_for_linux_and_unix_and_windows	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179268.	2020-07-01	not yet calculated	CVE-2020-4386 XF CONFIRM
ibm -- db2_for_linux_and_unix_and_windows	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local attacker to perform unauthorized actions on the system, caused by improper usage of shared memory. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information or cause a denial of service. IBM X-Force ID: 179989.	2020-07-01	not yet calculated	CVE-2020-4414 XF CONFIRM
ibm -- db2_for_linux_and_unix_and_windows	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated attacker to cause a denial of service due a hang in the execution of a terminate command. IBM X-Force ID: 180076.	2020-07-01	not yet calculated	CVE-2020-4420 XF CONFIRM
ibm -- db2_for_linux_and_unix_and_windows	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a	2020-07-01	not yet calculated	CVE-2020-4387 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179269.			CONFIRM
ibm -- db2_for_linux_and_unix_and_windows	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a denial of service, caused by improper handling of Secure Sockets Layer (SSL) renegotiation requests. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to increase the resource usage on the system. IBM X-Force ID: 178507.	2020-07-01	not yet calculated	CVE-2020-4355 XF CONFIRM
ibm -- db2_for_linux_and_unix_and_windows	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 178960.	2020-07-01	not yet calculated	CVE-2020-4363 XF CONFIRM
ibm -- mq_and_mq_appliance_and_mq_for_hpe_nonstop	IBM MQ, IBM MQ Appliance, IBM MQ for HPE NonStop 8.0.4 and 8.1.0 could allow an attacker to cause a denial of service caused by an error within the pubsub logic. IBM X-Force ID: 179081.	2020-07-01	not yet calculated	CVE-2020-4376 XF CONFIRM
ifax_solutions -- hylafax+_and_hylafax_enterprise	In HylaFAX+ through 7.0.2 and HylaFAX Enterprise, the	2020-06-30	not yet	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	faxsetup utility calls chown on files in user-owned directories. By winning a race, a local attacker could use this to escalate his privileges to root.		calculated	15396 MISC MISC
ifax_solutions -- hylafax+_and_hylafax_enterprise	HylaFAX+ through 7.0.2 and HylaFAX Enterprise have scripts that execute binaries from directories writable by unprivileged users (e.g., locations under /var/spool/hylafax that are writable by the uucp account). This allows these users to execute code in the context of the user calling these binaries (often root).	2020-06-30	not yet calculated	CVE-2020-15397 MISC MISC
iobit -- malware_fighter_pro	IOBit Malware Fighter Pro 8.0.2.547 allows local users to gain privileges for file deletion by manipulating malicious flagged file locations with an NTFS junction and an Object Manager symbolic link.	2020-06-30	not yet calculated	CVE-2020-15401 MISC
jenkins -- jenkins	Jenkins Link Column Plugin 1.0 and earlier does not filter URLs of links created by users with View/Configure permission, resulting in a stored cross-site scripting vulnerability.	2020-07-02	not yet calculated	CVE-2020-2219 MLIST CONFIRM
jenkins -- jenkins	Jenkins Sonargraph Integration Plugin 3.0.0 and earlier does not escape the file path for the Log file field form validation, resulting in a stored cross-site scripting vulnerability.	2020-07-02	not yet calculated	CVE-2020-2201 MLIST CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified username and password.	2020-07-02	not yet calculated	CVE-2020-2215 MLIST CONFIRM
jenkins -- jenkins	A missing permission check in Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified username and password.	2020-07-02	not yet calculated	CVE-2020-2216 MLIST CONFIRM
jenkins -- jenkins	Jenkins Compatibility Action Storage Plugin 1.0 and earlier does not escape the content coming from the MongoDB in the testConnection form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability.	2020-07-02	not yet calculated	CVE-2020-2217 MLIST CONFIRM
jenkins -- jenkins	Jenkins TestComplete support Plugin 2.4.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-07-02	not yet calculated	CVE-2020-2209 MLIST CONFIRM
jenkins -- jenkins	Jenkins Slack Upload Plugin 1.7 and earlier stores a secret unencrypted in job config.xml files on the Jenkins master where it can be viewed by users	2020-07-02	not yet calculated	CVE-2020-2208 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with Extended Read permission, or access to the master file system.			CONFIRM
jenkins -- jenkins	A missing permission check in Jenkins Fortify on Demand Plugin 6.0.0 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2020-07-02	not yet calculated	CVE-2020-2202 MLIST CONFIRM
jenkins -- jenkins	Jenkins HP ALM Quality Center Plugin 1.6 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-07-02	not yet calculated	CVE-2020-2218 MLIST CONFIRM
jenkins -- jenkins	Jenkins Stash Branch Parameter Plugin 0.3.0 and earlier transmits configured passwords in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	2020-07-02	not yet calculated	CVE-2020-2210 MLIST CONFIRM
jenkins -- jenkins	Jenkins VncRecorder Plugin 1.25 and earlier does not escape a tool path in the `checkVncServ` form validation endpoint, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by Jenkins administrators.	2020-07-02	not yet calculated	CVE-2020-2205 MLIST CONFIRM
jenkins -- jenkins	Jenkins GitHub Coverage Reporter Plugin 1.8 and earlier stores secrets unencrypted in its global configuration file on the	2020-07-02	not yet calculated	CVE-2020-2212 MLIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Jenkins master where they can be viewed by users with access to the master file system or read permissions on the system configuration.			T CONFIRM
jenkins -- jenkins	Jenkins ZAP Pipeline Plugin 1.9 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	2020-07-02	not yet calculated	CVE-2020-2214 MLIST CONFIRM
jenkins -- jenkins	Jenkins White Source Plugin 19.1.1 and earlier stores credentials unencrypted in its global configuration file and in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission (config.xml), or access to the master file system.	2020-07-02	not yet calculated	CVE-2020-2213 MLIST CONFIRM
jenkins -- jenkins	Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin 1.3 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	2020-07-02	not yet calculated	CVE-2020-2211 MLIST CONFIRM
jenkins -- jenkins	Jenkins VncViewer Plugin 1.7 and earlier does not escape a parameter value in the checkVncServ form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability.	2020-07-02	not yet calculated	CVE-2020-2207 MLIST CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins VncRecorder Plugin 1.25 and earlier does not escape a parameter value in the checkVncServ form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability.	2020-07-02	not yet calculated	CVE-2020-2206 MLIST CONFIRM
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Fortify on Demand Plugin 5.0.1 and earlier allows attackers to connect to the globally configured Fortify on Demand endpoint using attacker-specified credentials IDs.	2020-07-02	not yet calculated	CVE-2020-2203 MLIST CONFIRM
jenkins -- jenkins	A missing permission check in Jenkins Fortify on Demand Plugin 5.0.1 and earlier allows attackers with Overall/Read permission to connect to the globally configured Fortify on Demand endpoint using attacker-specified credentials IDs.	2020-07-02	not yet calculated	CVE-2020-2204 MLIST CONFIRM
journal -- journal	The Journal theme before 3.1.0 for OpenCart allows exposure of sensitive data via SQL errors.	2020-07-01	not yet calculated	CVE-2020-15478 MISC MISC MISC
klokan_technologies -- tileserver_gl	An issue was discovered in server.js in TileServer GL through 3.0.0. The content of the key GET parameter is reflected unsanitized in an HTTP response for the application's main page, causing reflected XSS.	2020-07-01	not yet calculated	CVE-2020-15500 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
koa-shopify-auth -- koa-shopify-auth	A cross-site scripting vulnerability exists in koa-shopify-auth v3.1.61-v3.1.62 that allows an attacker to inject JS payloads into the `shop` parameter on the `/shopify/auth/enable_cookies` endpoint.	2020-07-02	not yet calculated	CVE-2020-8176 MISC MISC
lead_technologies -- leadtools	An exploitable code execution vulnerability exists in the ANI file format parser of Leadtools 20. A specially crafted ANI file can cause a buffer overflow resulting in remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	2020-07-01	not yet calculated	CVE-2020-6089 MISC
libraw -- libraw	LibRaw before 0.20-Beta3 has an out-of-bounds write in parse_exif() in metadata\exif_gps.cpp via an unrecognized AtomName and a zero value of tiff_nifds.	2020-06-28	not yet calculated	CVE-2020-15365 MISC MISC
libraw -- libraw	LibRaw before 0.20-RC1 lacks a thumbnail size range check. This affects decoders/unpack_thumb.cpp, postprocessing/mem_image.cpp, and utils/thumb_utils.cpp. For example, malloc(sizeof(libraw_processed_image_t)+T.tlength) occurs without validating T.tlength.	2020-07-02	not yet calculated	CVE-2020-15503 MISC MISC MISC
libvncserver -- libvncserver	It was discovered that websockets.c in LibVNCServer prior to 0.9.12 did not properly decode certain WebSocket frames. A malicious attacker	2020-06-30	not yet calculated	CVE-2017-18922 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could exploit this by sending specially crafted WebSocket frames to a server, causing a heap-based buffer overflow.			MISC MISC MISC
linkplay_technology -- multiple_devices	An issue was discovered on various devices via the Linkplay firmware. There is WAN remote code execution without user interaction. An attacker could retrieve the AWS key from the firmware and obtain full control over Linkplay's AWS estate, including S3 buckets containing device firmware. When combined with an OS command injection vulnerability within the XML Parsing logic of the firmware update process, an attacker would be able to gain code execution on any device that attempted to update. Note that by default all devices tested had automatic updates enabled.	2020-07-01	not yet calculated	CVE-2019-15310 MISC MISC MISC
locutus -- locutus	php/exec/escapeshellarg in Locutus PHP through 2.0.11 allows an attacker to achieve code execution.	2020-07-01	not yet calculated	CVE-2020-13619 MISC MISC MISC
magento -- magento	XSS exists in the WebForms Pro M2 extension before 2.9.17 for Magento 2 via the textarea field.	2020-06-29	not yet calculated	CVE-2020-12635 MISC MISC
maipu -- mp_1800x_50_devices	The web interface of Maipu MP1800X-50 7.5.3.14(R) devices allows remote attackers to obtain sensitive information	2020-06-29	not yet calculated	CVE-2020-13896 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via the form/formDeviceVerGet URI, such as system id, hardware model, hardware version, bootloader version, software version, software image file, compilation time, and system uptime. This is similar to CVE-2019-1653.			
mavlink -- micro_air_vehicle_link_protocol	This vulnerability applies to the Micro Air Vehicle Link (MAVLink) protocol and allows a remote attacker to gain access to sensitive information provided it has access to the communication medium. MAVLink is a header-based protocol that does not perform encryption to improve transfer (and reception speed) and efficiency by design. The increasing popularity of the protocol (used accross different autopilots) has led to its use in wired and wireless mediums through insecure communication channels exposing sensitive information to a remote attacker with ability to intercept network traffic.	2020-07-03	not yet calculated	CVE-2020-10281 CONFIRM
mavlink -- micro_air_vehicle_link_protocol	The Micro Air Vehicle Link (MAVLink) protocol presents no authentication mechanism on its version 1.0 (nor authorization) whichs leads to a variety of attacks including identity spoofing, unauthorized access, PITM attacks and more. According to literature, version 2.0 optionally allows for package signing which mitigates this flaw. Another source	2020-07-03	not yet calculated	CVE-2020-10282 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mentions that MAVLink 2.0 only provides a simple authentication system based on HMAC. This implies that the flying system overall should add the same symmetric key into all devices of network. If not the case, this may cause a security issue, that if one of the devices and its symmetric key are compromised, the whole authentication system is not reliable.			
mcafee -- network_security_management	Exposure of Sensitive Information in McAfee Network Security Management (NSM) prior to 10.1.7.7 allows local users to gain unauthorised access to the root account via execution of carefully crafted commands from the restricted command line interface (CLI).	2020-07-03	not yet calculated	CVE-2020-7284 MISC
mcafee -- total_protection	Privilege Escalation vulnerability in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.	2020-07-03	not yet calculated	CVE-2020-7281 CONFIRM
mcafee -- total_protection	Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to delete files the user would	2020-07-03	not yet calculated	CVE-2020-7282 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine.			
mcafee -- total_protection	Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to create and edit files via symbolic link manipulation in a location they would otherwise not have access to. This is achieved through running a malicious script or program on the target machine.	2020-07-03	not yet calculated	CVE-2020-7283 CONFIRM
mirumee -- saleor_storefront	In Saleor Storefront before version 2.10.3, request data used to authenticate customers was inadvertently cached in the browser's local storage mechanism, including credentials. A malicious user with direct access to the browser could extract the email and password. In versions prior to 2.10.0 persisted the cache even after the user logged out. This is fixed in version 2.10.3. A workaround is to manually clear application data (browser's local storage) after logging into Saleor Storefront.	2020-06-30	not yet calculated	CVE-2020-15085 MISC MISC CONFIRM
misp -- misp	An issue was discovered in MISP 2.4.128. app/Controller/EventsController.php lacks an event ACL check	2020-06-30	not yet calculated	CVE-2020-15412 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	before proceeding to allow a user to send an event contact form.			
misp -- misp	An issue was discovered in MISP 2.4.128. app/Controller/AttributesController.php has insufficient ACL checks in the attachment downloader.	2020-06-30	not yet calculated	CVE-2020-15411 MISC
mitsubishi_electric -- multiple_fa_engineering_software_products	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N	2020-06-30	not yet calculated	CVE-2020-5602 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors.			
monsta -- monsta_ftp	Monsta FTP 2.10.1 or below allows external control of paths used in filesystem operations. This allows attackers to read and write arbitrary local files, allowing an attacker to gain remote code execution in common deployments.	2020-07-01	not yet calculated	CVE-2020-14057 MISC MISC
monsta -- monsta_ftp	Monsta FTP 2.10.1 or below is prone to a server-side request forgery vulnerability due to insufficient restriction of the web fetch functionality. This allows attackers to read arbitrary local files and interact with arbitrary third-party services.	2020-07-01	not yet calculated	CVE-2020-14056 MISC MISC
monsta -- monsta_ftp	Monsta FTP 2.10.1 or below is prone to a stored cross-site scripting vulnerability in the language setting due to insufficient output encoding.	2020-07-01	not yet calculated	CVE-2020-14055 MISC MISC
mversion -- mversion	The issue occurs because tagName user input is formatted inside the exec function is executed without any checks.	2020-07-01	not yet calculated	CVE-2020-7688 MISC MISC MISC
national_tax_agency -- e-tax	Chrome Extension for e-Tax Reception System Ver1.0.0.0	2020-06-30	not yet	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows remote attackers to execute an arbitrary command via unspecified vectors.		calculated	5601 MISC MISC
nedi_consulting -- nedi	NeDi 1.9C is vulnerable to Remote Command Execution. System-Snapshot.php improperly escapes shell metacharacters from a POST request. An attacker can exploit this by crafting an arbitrary payload (any system commands) that contains shell metacharacters via a POST request with a psw parameter. (This can also be exploited via CSRF.)	2020-06-29	not yet calculated	CVE-2020-14412 MISC
nedi_consulting -- nedi	NeDi 1.9C is vulnerable to Remote Command Execution. pwsec.php improperly escapes shell metacharacters from a POST request. An attacker can exploit this by crafting an arbitrary payload (any system commands) that contains shell metacharacters via a POST request with a pw parameter. (This can also be exploited via CSRF.)	2020-06-29	not yet calculated	CVE-2020-14414 MISC
nedi_consulting -- nedi	NeDi 1.9C is vulnerable to XSS because of an incorrect implementation of sanitize() in inc/libmisc.php. This function attempts to escape the SCRIPT tag from user-controllable values, but can be easily bypassed, as demonstrated by an onerror attribute of an IMG element as a Devices-Config.php?sta= value.	2020-06-29	not yet calculated	CVE-2020-14413 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netapp -- hci_h610s_baseboard_management_controller	The NetApp HCI H610S Baseboard Management Controller (BMC) is shipped with a documented default account and password that should be changed during the initial node setup. During upgrades to Element 11.8 and 12.0 the H610S BMC account password is reset to the default documented value which allows remote attackers to cause a Denial of Service (DoS).	2020-06-29	not yet calculated	CVE-2020-8573 MISC
nextcloud -- nextcloud_deck	Improper access control in Nextcloud Deck 1.0.0 allowed an attacker to inject tasks into other users decks.	2020-07-02	not yet calculated	CVE-2020-8179 MISC MISC
nginx -- nginx	In NGINX Controller 3.0.0-3.4.0, recovery code required to change a user's password is transmitted and stored in the database in plain text, which allows an attacker who can intercept the database connection or have read access to the database, to request a password reset using the email address of another registered user then retrieve the recovery code.	2020-07-01	not yet calculated	CVE-2020-5899 MISC
nginx -- nginx	In versions 3.0.0-3.4.0, 2.0.0-2.9.0, and 1.0.1, there is insufficient cross-site request forgery (CSRF) protections for the NGINX Controller user interface.	2020-07-01	not yet calculated	CVE-2020-5900 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nginx -- nginx	In NGINX Controller 3.3.0-3.4.0, undisclosed API endpoints may allow for a reflected Cross Site Scripting (XSS) attack. If the victim user is logged in as admin this could result in a complete compromise of the system.	2020-07-01	not yet calculated	CVE-2020-5901 MISC
nginx -- nginx	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, when users run the command displayed in NGINX Controller user interface (UI) to fetch the agent installer, the server TLS certificate is not verified.	2020-07-02	not yet calculated	CVE-2020-5909 MISC
nginx -- nginx	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the Neural Autonomic Transport System (NATS) messaging services in use by the NGINX Controller do not require any form of authentication, so any successful connection would be authorized.	2020-07-02	not yet calculated	CVE-2020-5910 MISC
nginx -- nginx	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the NGINX Controller installer starts the download of Kubernetes packages from an HTTP URL On Debian/Ubuntu system.	2020-07-02	not yet calculated	CVE-2020-5911 MISC
nozomi_networks -- guardian	Nozomi Guardian before 19.0.4 allows attackers to achieve stored XSS (in the web front end) by leveraging the ability to create a custom field with a crafted field name.	2020-06-30	not yet calculated	CVE-2020-15307 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nozomi_networks -- guardian_os	Nozomi Networks OS before 19.0.4 allows /#/network?tab=network_node_list.html CSV Injection.	2020-06-30	not yet calculated	CVE-2020-7049 MISC
ntop -- ndpi	In nDPI through 3.2, the Oracle protocol dissector has a heap-based buffer over-read in ndpi_search_oracle in lib/protocols/oracle.c.	2020-07-01	not yet calculated	CVE-2020-15476 MISC MISC
ntop -- ndpi	In nDPI through 3.2, the packet parsing code is vulnerable to a heap-based buffer over-read in ndpi_parse_packet_line_info in lib/ndpi_main.c.	2020-07-01	not yet calculated	CVE-2020-15471 MISC
ntop -- ndpi	In nDPI through 3.2, ndpi_reset_packet_line_info in lib/ndpi_main.c omits certain reinitialization, leading to a use-after-free.	2020-07-01	not yet calculated	CVE-2020-15475 MISC
ntop -- ndpi	In nDPI through 3.2, there is a stack overflow in extractRDNSequence in lib/protocols/tls.c.	2020-07-01	not yet calculated	CVE-2020-15474 MISC
ntop -- ndpi	In nDPI through 3.2, the OpenVPN dissector is vulnerable to a heap-based buffer over-read in ndpi_search_openvpn in lib/protocols/openvpn.c.	2020-07-01	not yet calculated	CVE-2020-15473 MISC
ntop -- ndpi	In nDPI through 3.2, the H.323 dissector is vulnerable to a heap-based buffer over-read in ndpi_search_h323 in lib/protocols/h323.c, as	2020-07-01	not yet calculated	CVE-2020-15472 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	demonstrated by a payload packet length that is too short.			
nvidia -- virtual_gpu_manager	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which the software does not restrict or incorrectly restricts operations within the boundaries of a resource that is accessed by using an index or pointer, such as memory or files, which may lead to code execution, denial of service, escalation of privileges, or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	2020-06-30	not yet calculated	CVE-2020-5968 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which an input data size is not validated, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	2020-06-30	not yet calculated	CVE-2020-5970 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which it validates a shared resource before using it, creating a race condition which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	2020-06-30	not yet calculated	CVE-2020-5969 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- virtual_gpu_manager	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which local pointer variables are not initialized and may be freed later, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	2020-06-30	not yet calculated	CVE-2020-5972 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which the software reads from a buffer by using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer, which may lead to code execution, denial of service, escalation of privileges, or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	2020-06-30	not yet calculated	CVE-2020-5971 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA Virtual GPU Manager and the guest drivers contain a vulnerability in vGPU plugin, in which there is the potential to execute privileged operations, which may lead to denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	2020-06-30	not yet calculated	CVE-2020-5973 CONFIRM UBUNTU UBUNTU
oauth2_proxy -- oauth2_proxy	In OAuth2 Proxy from version 5.1.1 and less than version 6.0.0, users can provide a redirect address for the proxy to send the	2020-06-29	not yet calculated	CVE-2020-4037 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated user to at the end of the authentication flow. This is expected to be the original URL that the user was trying to access. This redirect URL is checked within the proxy and validated before redirecting the user to prevent malicious actors providing redirects to potentially harmful sites. This has been fixed in version 6.0.0.			CONFIRM
objective_development_software -- little_snitch	Little Snitch version 4.5.1 and older changed ownership of a directory path controlled by the user. This allowed the user to escalate to root by linking the path to a directory containing code executed by root.	2020-06-30	not yet calculated	CVE-2020-13095 MISC
october -- october_cms	In October from version 1.0.319 and before version 1.0.467, pasting content copied from malicious websites into the Froala richeditor could result in a successful self-XSS attack. This has been fixed in 1.0.467.	2020-07-02	not yet calculated	CVE-2020-4061 MISC CONFIRM MISC
openbsd -- openssh	The client side in OpenSSH 5.7 through 8.3 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).	2020-06-29	not yet calculated	CVE-2020-14145 MISC MISC
openjpeg -- openjpeg	jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be	2020-06-29	not yet	CVE-2020-15389

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	triggered if there is a mix of valid and invalid files in a directory operated on by the decompressor. Triggering a double-free may also be possible. This is related to calling opj_image_destroy twice.		calculated	MISC MISC
palo_alto_networks -- pan-os	When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources. The attacker must have network access to the vulnerable server to exploit this vulnerability. This issue affects PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL). This issue does not affect PAN-OS 7.1. This issue cannot be exploited if SAML is not used for authentication. This issue cannot be exploited if the 'Validate Identity Provider Certificate' option is enabled (checked) in the SAML Identity Provider Server Profile. Resources that can be protected by SAML-based single sign-on (SSO) authentication are: GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN,	2020-06-29	not yet calculated	CVE-2020-2021 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Authentication and Captive Portal, PAN-OS next-generation firewalls (PA-Series, VM-Series) and Panorama web interfaces, Prisma Access In the case of GlobalProtect Gateways, GlobalProtect Portal, Clientless VPN, Captive Portal, and Prisma Access, an unauthenticated attacker with network access to the affected servers can gain access to protected resources if allowed by configured authentication and Security policies. There is no impact on the integrity and availability of the gateway, portal or VPN server. An attacker cannot inspect or tamper with sessions of regular users. In the worst case, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N). In the case of PAN-OS and Panorama web interfaces, this issue allows an unauthenticated attacker with network access to the PAN-OS or Panorama web interfaces to log in as an administrator and perform administrative actions. In the worst-case scenario, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). If the web interfaces are only accessible to a restricted management network, then the issue is lowered to a CVSS Base Score of 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). Palo			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Alto Networks is not aware of any malicious attempts to exploit this vulnerability.			
persian_vip_download_script -- persian_vip_download_script	Persian VIP Download Script 1.0 allows SQL Injection via the cart_edit.php active parameter.	2020-07-01	not yet calculated	CVE-2020-15468 MISC
phoenix_contact -- pc_worx_and_pc_worx_express	mwe file parsing in Phoenix Contact PC Worx and PC Worx Express version 1.87 and earlier is vulnerable to out-of-bounds read remote code execution. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation.	2020-07-01	not yet calculated	CVE-2020-12498 CONFIRM
phoenix_contact -- pc_worx_and_pc_worx_express	PLCopen XML file parsing in Phoenix Contact PC Worx and PC Worx Express version 1.87 and earlier can lead to a stack-based overflow. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation.	2020-07-01	not yet calculated	CVE-2020-12497 CONFIRM
powerdns -- recursor	In PowerDNS Recursor versions up to and including 4.3.1, 4.2.2 and 4.1.16, the ACL restricting access to the internal web server is not properly enforced.	2020-07-01	not yet calculated	CVE-2020-14196 CONFIRM CONFIRM
prestashop -- prestashop	In PrestaShop from version 1.7.4.0 and before version 1.7.6.6, some files should not be in the release archive, and others	2020-07-02	not yet calculated	CVE-2020-15080 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	should not be accessible. The problem is fixed in version 1.7.6.6 A possible workaround is to make sure `composer.json` and `docker-compose.yml` are not accessible on your server.			CONFIRM
prestashop -- prestashop	In PrestaShop from version 1.5.0.0 and before version 1.7.6.6, there is improper access control in Carrier page, Module Manager and Module Positions. The problem is fixed in version 1.7.6.6	2020-07-02	not yet calculated	CVE-2020-15079 MISC CONFIRM
presto -- presto	In Presto before version 337, authenticated users can bypass authorization checks by directly accessing internal APIs. This impacts Presto server installations with secure internal communication configured. This does not affect installations that have not configured secure internal communication, as these installations are inherently insecure. This only affects Presto server installations. This does NOT affect clients such as the CLI or JDBC driver. This vulnerability has been fixed in version 337. Additionally, this issue can be mitigated by blocking network access to internal APIs on the coordinator and workers.	2020-06-30	not yet calculated	CVE-2020-15087 CONFIRM MISC
putty -- putty	PuTTY 0.68 through 0.73 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle	2020-06-29	not yet calculated	CVE-2020-14002 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to target initial connection attempts (where no host key for the server has been cached by the client).			MISC MISC
python -- python	In Python 3.6 through 3.6.10, 3.7 through 3.7.8, 3.8 through 3.8.4rc1, and 3.9 through 3.9.0b4 on Windows, a Trojan horse python3.dll might be used in cases where CPython is embedded in a native application. This occurs because python3X.dll may use an invalid search path for python3.dll loading (after Py_SetPath has been used). NOTE: this issue CANNOT occur when using python.exe from a standard (non-embedded) Python installation on Windows.	2020-07-04	not yet calculated	CVE-2020-15523 MISC MISC
qemu -- qemu	In QEMU 4.2.0, a MemoryRegionOps object may lack read/write callback methods, leading to a NULL pointer dereference.	2020-07-02	not yet calculated	CVE-2020-15469 CONFIRM MISC
qnap -- kayako_service	This improper access control vulnerability in Helpdesk allows attackers to get control of QNAP Kayako service. Attackers can access the sensitive data on QNAP Kayako server with API keys. We have replaced the API key to mitigate the vulnerability, and already fixed the issue in Helpdesk 3.0.1 and later versions.	2020-07-01	not yet calculated	CVE-2020-2500 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rack -- rack	A directory traversal vulnerability exists in rack < 2.2.0 that allows an attacker perform directory traversal vulnerability in the Rack::Directory app that is bundled with Rack which could result in information disclosure.	2020-07-02	not yet calculated	CVE-2020-8161 MISC MISC
red_hat -- ceph_storage_radosgw	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway). The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. Ceph versions 3.x and 4.x are vulnerable to this issue.	2020-06-26	not yet calculated	CVE-2020-10753 SUSE CONFIRM FEDORA
ruby_on_rails -- ruby_on_rails	The is a code injection vulnerability in versions of Rails prior to 5.0.1 that wouldallow an attacker who controlled the `locals` argument of a `render` call to perform a RCE.	2020-07-02	not yet calculated	CVE-2020-8163 MISC MISC
ruby_on_rails -- ruby_on_rails	A denial of service vulnerability exists in Rails <6.0.3.2 that allowed an untrusted user to run any pending migrations on a Rails app running in production.	2020-07-02	not yet calculated	CVE-2020-8185 MISC MISC
ruby_on_rails -- ruby_on_rails	A CSRF forgery vulnerability exists in rails < 5.2.5, rails < 6.0.4 that makes it possible for an attacker to, given a global CSRF token such as the one present in the authenticity_token	2020-07-02	not yet calculated	CVE-2020-8166 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	meta tag, forge a per-form CSRF token.			
sap -- solution_manager	SAP Solution Manager (Trace Analysis), version 7.20, allows an attacker to perform a log injection into the trace file, due to Incomplete XML Validation. The readability of the trace file is impaired.	2020-07-01	not yet calculated	CVE-2020-6261 MISC MISC
sophos -- xg_firewall	Sophos XG Firewall 17.x through v17.5 MR12 allows a Buffer Overflow and remote code execution via the HTTP/S Bookmarks feature for clientless access. Hotfix HF062020.1 was published for all firewalls running v17.x.	2020-06-29	not yet calculated	CVE-2020-15069 CONFIRM
squid -- squid	An issue was discovered in Squid before 4.12 and 5.x before 5.0.3. Due to use of a potentially dangerous function, Squid and the default certificate validation helper are vulnerable to a Denial of Service when opening a TLS connection to an attacker-controlled server for HTTPS. This occurs because unrecognized error values are mapped to NULL, but later code expects that each error value is mapped to a valid error string.	2020-06-30	not yet calculated	CVE-2020-14058 CONFIRM MISC MISC
squid -- squid	An issue was discovered in Squid 5.x before 5.0.3. Due to an Incorrect Synchronization, a Denial of Service can occur when processing objects in an SMP cache because of an Ipc::Mem::PageStack::pop ABA	2020-06-30	not yet calculated	CVE-2020-14059 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	problem during access to the memory page/slot management list.			
squid -- squid	An issue was discovered in http/ContentLengthInterpreter.cc in Squid before 4.12 and 5.x before 5.0.3. A Request Smuggling and Poisoning attack can succeed against the HTTP cache. The client sends an HTTP request with a Content-Length header containing "+\ "-" or an uncommon shell whitespace character prefix to the length field-value.	2020-06-30	not yet calculated	CVE-2020-15049 MISC MISC CONFIRM
suse -- multiple_products	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of kopano-spamd of openSUSE Leap 15.1, openSUSE Tumbleweed allowed local attackers with the privileges of the kopano user to escalate to root. This issue affects: openSUSE Leap 15.1 kopano-spamd versions prior to 10.0.5-lp151.4.1. openSUSE Tumbleweed kopano-spamd versions prior to 10.0.5-1.1.	2020-06-29	not yet calculated	CVE-2020-8014 CONFIRM
suse -- multiple_products	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3,	2020-06-29	not yet calculated	CVE-2020-8019 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1.			
suse -- multiple_products	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE	2020-06-29	not yet calculated	CVE-2020-8022 SUSE CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.			
suse -- multiple_products	A Incorrect Default Permissions vulnerability in the packaging of hylafax+ of openSUSE Leap 15.2, openSUSE Leap 15.1, openSUSE Factory allows local attackers to escalate from user uucp to users calling hylafax binaries. This issue affects: openSUSE Leap 15.2 hylafax+ versions prior to 7.0.2-lp152.2.1. openSUSE Leap 15.1 hylafax+ version 5.6.1-lp151.3.7 and prior versions. openSUSE Factory hylafax+ versions prior to 7.0.2-2.1.	2020-06-29	not yet calculated	CVE-2020-8024 CONFIRM
suse -- multiple_products	A External Control of File Name or Path vulnerability in osc of SUSE Linux Enterprise Module for Development Tools 15, SUSE Linux Enterprise Software Development Kit 12-SP5, SUSE Linux Enterprise Software Development Kit 12-SP4; openSUSE Leap 15.1, openSUSE Factory allowed remote attackers that can change downloaded packages to overwrite arbitrary files. This issue affects: SUSE Linux Enterprise Module for Development Tools 15 osc versions prior to 0.169.1-3.20.1. SUSE Linux Enterprise Software Development Kit 12-SP5 osc versions prior to	2020-06-29	not yet calculated	CVE-2019-3681 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	0.162.1-15.9.1. SUSE Linux Enterprise Software Development Kit 12-SP4 osc versions prior to 0.162.1-15.9.1. openSUSE Leap 15.1 osc versions prior to 0.169.1-lp151.2.15.1. openSUSE Factory osc versions prior to 0.169.0 .			
synacor -- zimbra_collaboration_suite	An XSS vulnerability exists in the Webmail component of Zimbra Collaboration Suite before 8.8.15 Patch 11. It allows an attacker to inject executable JavaScript into the account name of a user's profile. The injected code can be reflected and executed when changing an e-mail signature.	2020-07-02	not yet calculated	CVE-2020-13653 MISC CONFIRM MISC MISC
tendermint -- tendermint	TenderMint from version 0.33.0 and before version 0.33.6 allows block proposers to include signatures for the wrong block. This may happen naturally if you start a network, have it run for some time and restart it (**without changing chainID**). A malicious block proposer (even with a minimal amount of stake) can use this vulnerability to completely halt the network. This issue is fixed in Tendermint 0.33.6 which checks all the signatures are for the block with 2/3+ majority before creating a commit.	2020-07-02	not yet calculated	CVE-2020-15091 MISC MISC CONFIRM
thingsdk -- wifi_scanner	wifiscanner.js in thingsSDK WiFi Scanner 1.0.1 allows Code Injection because it can be used with options to overwrite the	2020-06-29	not yet calculated	CVE-2020-15362 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	default executable/binary path and its arguments. An attacker can abuse this functionality to execute arbitrary code.			
tibco_software -- multiple_products	The MFT Browser file transfer client and MFT Browser admin client components of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contain a vulnerability that theoretically allows an attacker to craft an URL that will execute arbitrary commands on the affected system. If the attacker convinces an authenticated user with a currently active session to enter or click on the URL the commands will be executed on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions 8.2.1 and below.	2020-06-30	not yet calculated	CVE-2020-9413 CONFIRM
tibco_software -- multiple_products	The MFT admin service component of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contains a vulnerability that theoretically allows an authenticated user with specific permissions to obtain the session identifier of another user. The session identifier when replayed could provide administrative rights or	2020-06-30	not yet calculated	CVE-2020-9414 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	file transfer permissions to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions 8.2.1 and below.			
tobesoft -- cymiinstaller322	CyMiInstaller322 ActiveX which runs MIPLATFORM downloads files required to run applications. A vulnerability in downloading files by CyMiInstaller322 ActiveX caused by an attacker to download randomly generated DLL files and MIPLATFORM to load those DLLs due to insufficient verification.	2020-06-30	not yet calculated	CVE-2019-19161 MISC MISC
tobesoft -- nexacro14/17_excommonapiv13	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by setting the arguments to the vulnerable API. This can be leveraged for code execution by rebooting the victim’s PC	2020-07-02	not yet calculated	CVE-2020-7820 CONFIRM CONFIRM
tobesoft -- nexacro14/17_excommonapiv13	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by modifying the value of registry path. This can be leveraged for code execution by rebooting the victim’s PC	2020-07-02	not yet calculated	CVE-2020-7821 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
unifi -- protect	We have recently released new version of UniFi Protect firmware v1.13.3 and v1.14.10 for Unifi Cloud Key Gen2 Plus and UniFi Dream Machine Pro/UNVR respectively that fixes vulnerabilities found on Protect firmware v1.13.2, v1.14.9 and prior according to the description below:View only users can run certain custom commands which allows them to assign themselves unauthorized roles and escalate their privileges.	2020-07-02	not yet calculated	CVE-2020-8188 MISC MISC MISC
veeam_software -- veeam_availability_suite	VeeamFSR.sys in Veeam Availability Suite before 10 and Veeam Backup & Replication before 10 has no device object DACL, which allows unprivileged users to achieve total control over filesystem I/O requests.	2020-07-03	not yet calculated	CVE-2020-15518 MISC
wavlink -- wl-wn530hg4_devices	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple shell metacharacter injection vulnerabilities exist in CGI scripts, leading to remote code execution with root privileges.	2020-07-01	not yet calculated	CVE-2020-15489 MISC
wavlink -- wl-wn530hg4_devices	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple buffer overflow vulnerabilities exist in CGI scripts, leading to remote code execution with root privileges. (The set of affected	2020-07-01	not yet calculated	CVE-2020-15490 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	scripts is similar to CVE-2020-12266.)			
windows_cleaning_assistant -- windows_cleaning_assistant	In Windows cleaning assistant 3.2, the driver file (AtpKrnl.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x223CCD.	2020-06-30	not yet calculated	CVE-2020-14957 MISC MISC
windows_cleaning_assistant -- windows_cleaning_assistant	In Windows cleaning assistant 3.2, the driver file (AtpKrnl.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x223CCA.	2020-06-30	not yet calculated	CVE-2020-14956 MISC MISC
wordpress -- wordpress	The CodePeople Payment Form for PayPal Pro plugin before 1.1.65 for WordPress allows SQL Injection.	2020-07-02	not yet calculated	CVE-2020-14092 MISC MISC MISC
xrdp-sesman -- xrdp-sesman	The xrdp-sesman service before version 0.9.13.1 can be crashed by connecting over port 3350 and supplying a malicious payload. Once the xrdp-sesman process is dead, an unprivileged attacker on the server could then proceed to start their own imposter sesman service listening on port 3350. This will allow them to capture any user credentials that are submitted to XRDP and approve or reject arbitrary login credentials. For	2020-06-30	not yet calculated	CVE-2020-4044 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	xorgxrdp sessions in particular, this allows an unauthorized user to hijack an existing session. This is a buffer overflow attack, so there may be a risk of arbitrary code execution as well.			
zolo -- halo_devices	An issue was discovered on Zolo Halo devices via the Linkplay firmware. There is a Zolo Halo DNS rebinding attack. The device was found to be vulnerable to DNS rebinding. Combined with one of the many /httpapi.asp endpoint command-execution security issues, the DNS rebinding attack could allow an attacker to compromise the victim device from the Internet.	2020-07-01	not yet calculated	CVE-2019-15312 MISC MISC MISC
zolo -- halo_devices	An issue was discovered on Zolo Halo devices via the Linkplay firmware. There is Zolo Halo LAN remote code execution. The Zolo Halo Bluetooth speaker had a GoAhead web server listening on the port 80. The /httpapi.asp endpoint of the GoAhead web server was also vulnerable to multiple command execution vulnerabilities.	2020-07-01	not yet calculated	CVE-2019-15311 MISC MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account within the /opt/axess chroot directory tree.	2020-06-29	not yet calculated	CVE-2020-15315 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the cloud1234 password for the	2020-06-29	not yet	CVE-2020-15323

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a1@chopin account default credentials.		calculated	MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account within the /opt/mysql chroot directory tree.	2020-06-29	not yet calculated	CVE-2020-15318 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded ECDSA SSH key for the root account within the /opt/axess chroot directory tree.	2020-06-29	not yet calculated	CVE-2020-15316 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account within the /opt/axess chroot directory tree.	2020-06-29	not yet calculated	CVE-2020-15317 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the axzyxel password for the livedbuser account.	2020-06-29	not yet calculated	CVE-2020-15321 MISC MISC
zyxel -- cloudcnm_secumanager	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the wbboEZ4BN3ssxAfM hardcoded password for the debian-sys-maint account.	2020-06-29	not yet calculated	CVE-2020-15322 MISC MISC