Vulnerability Summary for the Week of July 1, 2019

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

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

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

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- web6000q_firmware	On Telus Actiontec WEB6000Q v1.1.02.22 devices, an attacker can login with root level access with the user "root" and password "admin" by using the enabled onboard UART headers.	2019-06-28	10.0	CVE-2018-15555 MISC FULLDISC
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple heap-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow	2019-06-28	7.5	CVE-2019-10989 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote code execution. Note: A different vulnerability than CVE-2019-10991.			
advantech -- webaccess	In WebAccess/SCADA, Versions 8.3.5 and prior, multiple stack-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	7.5	CVE-2019-10991 MISC MISC MISC MISC MISC MISC MISC MISC
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple untrusted pointer dereference vulnerabilities may allow a remote attacker to execute arbitrary code.	2019-06-28	7.5	CVE-2019-10993 MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chamilo -- chamilo_lms	Chamilo LMS 1.11.8 and 2.x allows remote code execution through an lp_upload.php unauthenticated file upload feature. It extracts a ZIP archive before checking its content, and once it has been extracted, does not check files in a recursive way. This means that by putting a .php file in a folder and then this folder in a ZIP archive, the server will accept this file without any checks. Because one can access this file from the website, it is remote code execution. This is related to a scorm imsmanifest.xml file, the import_package function, and extraction in $courseSysDir.$newDir.	2019-06-30	7.5	CVE-2019-13082 MISC MISC
cszcms -- csz_cms	core/MY_Security.php in CSZ CMS 1.2.2 before 2019-06-20 has member/login/check SQL injection by sending a crafted HTTP User-Agent header and omitting the csrf_csz parameter.	2019-06-30	7.5	CVE-2019-13086 MISC
dosbox -- dosbox	DOSBox 0.74-2 has Incorrect Access Control.	2019-07-02	7.5	CVE-2019-12594 CONFIRM MLIST FEDOR

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				A MISC MISC
flowpaper -- flexpaper	The Publish Service in FlexPaper (later renamed FlowPaper) 2.3.6 allows remote code execution via setup.php and change_config.php.	2019-07-03	7.5	CVE-2018-11686 MISC MISC
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 could allow malicious user with access to the DB2 instance account to leverage a fenced execution process to execute arbitrary code as root. IBM X-Force ID: 156567.	2019-07-01	7.2	CVE-2019-4057 XF CONFIRM
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 158519.	2019-07-01	7.2	CVE-2019-4154 BID XF CONFIRM
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1,	2019-07-01	7.2	CVE-2019-4322

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 161202.			BID XF CONFIRM
icon -- loopchain	In Loopchain through 2.2.1.3, an attacker can escalate privileges from a low-privilege shell by changing the environment (aka injection in the DEFAULT_SCORE_HOST environment variable).	2019-06-28	9.0	CVE-2019-12997 MISC
lexmark -- 6500_firmware	Various Lexmark devices have a Buffer Overflow (issue 1 of 2).	2019-06-28	7.5	CVE-2018-15519 CONFIRM
lexmark -- cx421_firmware	Various Lexmark devices have a Buffer Overflow (issue 2 of 2).	2019-06-28	7.5	CVE-2018-15520 CONFIRM
matio_project -- matio	Multiple integer overflows exist in MATIO before 1.5.16, related to mat.c, mat4.c, mat5.c, mat73.c, and matvar_struct.c	2019-06-30	7.5	CVE-2019-13107 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netapp -- clustered_data_ontap	NetApp AFF A700s Baseboard Management Controller (BMC) firmware versions 1.22 and higher were shipped with a default account enabled that could allow unauthorized arbitrary command execution.	2019-07-01	7.5	CVE-2019-5497 CONFIRM
nginx -- njs	njs through 0.3.3, used in NGINX, has a buffer over-read in nxt_utf8_decode in nxt/nxt_utf8.c. This issue occurs after the fix for CVE-2019-12207 is in place.	2019-06-29	7.5	CVE-2019-13067 MISC
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Authentication Bypass.	2019-07-02	7.5	CVE-2019-7266 MISC MISC
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Authenticated Command Injection with root Code Execution.	2019-07-02	10.0	CVE-2019-7269 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Directory Traversal.	2019-07-02	7.5	CVE-2019-7253 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow File Inclusion.	2019-07-02	9.0	CVE-2019-7254 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Command Injections.	2019-07-02	10.0	CVE-2019-7256 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Unrestricted File Upload.	2019-07-02	7.5	CVE-2019-7257 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Hard-coded Credentials.	2019-07-02	10.0	CVE-2019-7261 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have a Version Control Failure.	2019-07-02	10.0	CVE-2019-7263 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow a Stack-based Buffer Overflow on the ARM platform.	2019-07-02	7.5	CVE-2019-7264 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Remote Code Execution (root access over SSH).	2019-07-02	10.0	CVE-2019-7265 MISC MISC
odoo -- odoo	Incorrect access control in the database manager component in Odoo Community 10.0 and 11.0 and Odoo Enterprise 10.0 and 11.0 allows a remote attacker to restore a database dump without knowing the super-admin password. An arbitrary password succeeds.	2019-06-28	7.5	CVE-2018-14885 MISC CONFIRM
optergy -- enterprise	Optergy Proton/Enterprise devices allow Authenticated File Upload with Code Execution as root.	2019-07-01	10.0	CVE-2019-7274 BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Remote Root Code Execution via a Backdoor Console.	2019-07-01	10.0	CVE-2019-7276 BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices have Hard-coded Credentials.	2019-07-01	7.5	CVE-2019-7279 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
primasystems -- flexair	Prima Systems FlexAir devices allow Unauthenticated Command Injection resulting in Root Remote Code Execution.	2019-07-01	10.0	CVE-2019-7669 MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices allow Authenticated Command Injection resulting in Root Remote Code Execution.	2019-07-01	9.0	CVE-2019-7670 MISC MISC
pulsesecure -- pulse_connect_secure	Session data between cluster nodes during cluster synchronization is not properly encrypted in Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX, PPS 5.2RX, or stand-alone devices.	2019-06-28	7.5	CVE-2018-20810 CONFIRM
pulsesecure -- pulse_connect_secure	An input validation issue has been found with login_meeting.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2.	2019-06-28	7.5	CVE-2018-20813 CONFIRM
redhat -- satellite	A path traversal flaw was found in spacewalk-proxy, all versions through 2.9, in the way the proxy processes cached client tokens. A remote, unauthenticated	2019-07-02	7.5	CVE-2019-10137 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker could use this flaw to test the existence of arbitrary files, if they have access to the proxy's filesystem, or can execute arbitrary code in the context of the httpd process.			
synology -- calendar	OS command injection vulnerability in drivers_syno_import_user.php in Synology Calendar before 2.3.1-0617 allows remote attackers to execute arbitrary commands via the crafted 'X-Real-IP' header.	2019-06-30	7.5	CVE-2019-11829 CONFIRM
synology -- photo_station	SQL injection vulnerability in synophoto_csPhotoDB.php in Synology Photo Station before 6.8.11-3489 and before 6.3-2977 allows remote attackers to execute arbitrary SQL command via the type parameter.	2019-06-30	7.5	CVE-2019-11821 CONFIRM
toaruos -- toaruos	linker/linker.c in ToaruOS through 1.10.9 has insecure LD_LIBRARY_PATH handling in setuid applications.	2019-06-29	7.2	CVE-2019-13046 MISC
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 has incorrect access control in sys_sysfunc case 9 for TOARU_SYS_FUNC_SETH	2019-06-29	7.2	CVE-2019-13047 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	EAP, allowing arbitrary kernel pages to be mapped into user land, leading to root access.			
toaruos -- toaruos	An integer wrap in kernel/sys/syscall.c in ToaruOS 1.10.10 allows users to map arbitrary kernel pages into userland process space via TOARU_SYS_FUNC_MMAP, leading to escalation of privileges.	2019-06-29	7.2	CVE-2019-13049 MISC
web-gooroo -- cms_web-gooroo	SQL injection vulnerability in /wbg/core/_includes/authorization.inc.php in CMS Web-Gooroo through 2013-01-19 allows remote attackers to execute arbitrary SQL commands via the wbg_login parameter.	2019-07-03	7.5	CVE-2017-18346 MISC EXPLOIT-DB

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acdsee -- acdsee	ACDSee Free 1.1.21 has a User Mode Write AV starting at	2019-07-04	6.8	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	IDE_ACDStd!JPEGTransW+0x000 00000000024ed.			13247 MISC
acdsee -- acdsee	ACDSee Free 1.1.21 has a User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x000 0000000002450.	2019-07-04	6.8	CVE-2019-13248 MISC
acdsee -- acdsee	ACDSee Free 1.1.21 has a User Mode Write AV starting at IDE_ACDStd!IEP_SetColorProfile +0x00000000000b9e7a.	2019-07-04	6.8	CVE-2019-13249 MISC
acdsee -- acdsee	ACDSee Free 1.1.21 has a User Mode Write AV starting at IDE_ACDStd!IEP_SetColorProfile +0x00000000000b9c2f.	2019-07-04	6.8	CVE-2019-13250 MISC
acdsee -- acdsee	ACDSee Free 1.1.21 has a User Mode Write AV starting at IDE_ACDStd!IEP_SetColorProfile +0x00000000000c47ff.	2019-07-04	6.8	CVE-2019-13251 MISC
acdsee -- acdsee	ACDSee Free 1.1.21 has a User Mode Write AV starting at IDE_ACDStd!IEP_SetColorProfile +0x00000000001172b0.	2019-07-04	6.8	CVE-2019-13252 MISC
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, an out-of-bounds read vulnerability is caused by a lack of proper validation of user-supplied data. Exploitation of this vulnerability may allow disclosure of information.	2019-06-28	5.0	CVE-2019-10983 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- webaccess	In WebAccess/SCADA, Versions 8.3.5 and prior, a path traversal vulnerability is caused by a lack of proper validation of a user-supplied path prior to use in file operations. An attacker can leverage this vulnerability to delete files while posing as an administrator.	2019-06-28	6.4	CVE-2019-10985 MISC MISC
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple out-of-bounds write vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	6.8	CVE-2019-10987 MISC MISC MISC
advisto -- peel_shopping	Advisto PEEL SHOPPING 9.0.0 has CSRF via en/achat/caddie_ajout.php and en/achat/caddie_affichage.php, as demonstrated by an XSS payload in the couleurId[0] parameter to the latter.	2019-06-30	6.8	CVE-2018-20848 MISC
arastta -- ecommerce	Arastta eCommerce 1.6.2 is vulnerable to XSS via the PATH_INFO to the login/ URI.	2019-06-30	4.3	CVE-2018-20849 MISC
archon_project -- archon	packages/subjects/pub/subjects.php in Archon 3.21 rev-1 has XSS in the referer parameter in an index.php?subjecttypeid=xxx	2019-07-03	4.3	CVE-2017-17972 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	request, aka Open Bug Bounty ID OBB-466362.			
audio_file_library_project -- audio_file_library	In Audio File Library (aka audiofile) 0.3.6, there exists one NULL pointer dereference bug in ulaw2linear_buf in G711.cpp in libmodules.a that allows an attacker to cause a denial of service via a crafted file.	2019-07-01	4.3	CVE-2019-13147 MISC
cyberpanel -- cyberpanel	An issue was discovered in CyberPanel through 1.8.4. On the user edit page, an attacker can edit the administrator's e-mail and password because of the lack of CSRF protection.	2019-07-02	6.8	CVE-2019-13056 MISC MISC
elitecms -- elite_cms	An issue was discovered in Elite CMS Pro 2.01. In /admin/add_sidebar.php, the ?page= parameter is vulnerable to SQL injection.	2019-07-03	6.5	CVE-2018-12250 MISC MISC
exiv2 -- exiv2	An integer overflow in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted PNG image file, because PngImage::readMetadata mishandles a zero value for iccOffset.	2019-06-30	4.3	CVE-2019-13108 MISC MISC
exiv2 -- exiv2	An integer overflow in Exiv2 through 0.27.1 allows an attacker to cause a denial of service	2019-06-30	4.3	CVE-2019-13109

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(SIGSEGV) via a crafted PNG image file, because PngImage::readMetadata mishandles a chunkLength - iccOffset subtraction.			MISC MISC
exiv2 -- exiv2	A CiffDirectory::readDirectory integer overflow and out-of-bounds read in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted CRW image file.	2019-06-30	4.3	CVE-2019-13110 MISC MISC
exiv2 -- exiv2	A WebPImage::decodeChunks integer overflow in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (large heap allocation followed by a very long running loop) via a crafted WEBP image file.	2019-06-30	4.3	CVE-2019-13111 MISC MISC
exiv2 -- exiv2	A PngChunk::parseChunkContent uncontrolled memory allocation in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (crash due to an std::bad_alloc exception) via a crafted PNG image file.	2019-06-30	4.3	CVE-2019-13112 MISC MISC
exiv2 -- exiv2	Exiv2 through 0.27.1 allows an attacker to cause a denial of service (crash due to assertion failure) via an invalid data location in a CRW image file.	2019-06-30	4.3	CVE-2019-13113 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
exiv2 -- exiv2	http.c in Exiv2 through 0.27.1 allows a malicious http server to cause a denial of service (crash due to a NULL pointer dereference) by returning a crafted response that lacks a space character.	2019-06-30	4.3	CVE-2019-13114 MISC MISC
f5 -- big-ip_access_policy_manager	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.5, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4 and BIG-IQ 6.0.0-6.1.0 and 5.1.0-5.4.0, an undisclosed iControl REST worker vulnerable to command injection for an Administrator user.	2019-07-02	6.5	CVE-2019-6620 CONFIRM
f5 -- big-ip_access_policy_manager	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.5, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, 11.6.1-11.6.3.4, and 11.5.1-11.5.8 and BIG-IQ 6.0.0-6.1.0 and 5.1.0-5.4.0, an undisclosed iControl REST worker is vulnerable to command injection by an admin/resource admin user. This issue impacts both iControl REST and tmsh implementations.	2019-07-02	6.5	CVE-2019-6621 CONFIRM
f5 -- big-ip_access_policy_manager	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.5, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4, an undisclosed iControl REST worker is vulnerable to command injection by an administrator or resource administrator user. This attack is only exploitable on multi-bladed systems.	2019-07-02	6.5	CVE-2019-6622 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip_access_policy_manager	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, undisclosed traffic sent to BIG-IP iSession virtual server may cause the Traffic Management Microkernel (TMM) to restart, resulting in a Denial-of-Service (DoS).	2019-07-02	5.0	CVE-2019-6623 BID CONFIRM
f5 -- big-ip_access_policy_manager	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, an undisclosed traffic pattern sent to a BIG-IP UDP virtual server may lead to a denial-of-service (DoS).	2019-07-02	5.0	CVE-2019-6624 CONFIRM
f5 -- websafe_alert_server	A Cross Site Scripting (XSS) vulnerability in versions of F5 WebSafe Dashboard 3.9.x and earlier, aka F5 WebSafe Alert Server, allows an unauthenticated user to inject HTML via a crafted alert.	2019-07-01	4.3	CVE-2016-5235 CONFIRM
fla-shop -- html5_maps	Cross-site request forgery (CSRF) vulnerability in HTML5 Maps 1.6.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5983 MISC MISC
flightcrew_project -- flightcrew	An issue was discovered in FlightCrew v0.9.2 and earlier. A NULL pointer dereference occurs in GetRelativePathToNcx() or GetRelativePathsToXhtmlDocumen	2019-06-28	4.3	CVE-2019-13032 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ts() when a NULL pointer is passed to xc::XMLUri::isValidURI(). This affects third-party software (not Sigil) that uses FlightCrew as a library.			
gnome -- glib	The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.59.1 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used. This is similar to CVE-2019-12450.	2019-06-28	5.0	CVE-2019-13012 MISC MISC MISC
grafana -- grafana	public/app/features/panel/panel_ctrl.ts in Grafana before 6.2.5 allows HTML Injection in panel drilldown links (via the Title or url field).	2019-06-29	4.3	CVE-2019-13068 MISC MISC
ibm -- bigfix_inventory	IBM BigFix Inventory v9 (SUA v9 / ILMT v9) discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161807.	2019-06-28	5.0	CVE-2019-4369 CONFIRM BID XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- daeja_viewone	IBM Daeja ViewONE Professional, Standard & Virtual 5.0 through 5.0.5 could allow an unauthorized user to download server files resulting in sensitive information disclosure. IBM X-Force ID: 160012.	2019-07-02	5.0	CVE-2019-4260 CONFIRM XF
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158092.	2019-07-01	4.3	CVE-2019-4102 BID XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158281.	2019-07-02	4.3	CVE-2019-4134 XF CONFIRM
ibm -- security_guardium	IBM Security Guardium 10.5 could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable web server. IBM X-Force ID: 160698.	2019-07-02	6.5	CVE-2019-4292 BID XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console could allow a remote attacker to obtain sensitive information when a specially crafted url causes a stack trace to be dumped. IBM X-Force ID: 160202.	2019-06-28	5.0	CVE-2019-4269 BID XF CONFIRM
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadBMPImage in coders/bmp.c.	2019-07-01	4.3	CVE-2019-13133 MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadVIFFImage in coders/viff.c.	2019-07-01	4.3	CVE-2019-13134 MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability in the function ReadCUTImage in coders/cut.c.	2019-07-01	6.8	CVE-2019-13135 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has an integer overflow vulnerability in the function TIFFSeekCustomStream in coders/tiff.c.	2019-07-01	6.8	CVE-2019-13136 MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the	2019-07-01	4.3	CVE-2019-13137

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	function ReadPSImage in coders/ps.c.			MISC MISC MISC
intelliants -- subrion	Subrion CMS before 4.1.4 has XSS.	2019-07-03	4.3	CVE-2018-11317 MISC CONFIRM
irssi -- irssi	Irssi before 1.0.8, 1.1.x before 1.1.3, and 1.2.x before 1.2.1, when SASL is enabled, has a use after free when sending SASL login to the server.	2019-06-29	6.8	CVE-2019-13045 SUSE MISC MLIST BID MISC MISC BUGTRAQ UBUNTU
istio -- istio	Istio before 1.2.2 mishandles certain access tokens, leading to "Epoch 0 terminated with an error" in Envoy. This is related to a jwt_authenticator.cc segmentation fault.	2019-06-28	5.0	CVE-2019-12995 MISC MISC MISC
jetbrains -- teamcity	A reflected XSS on a user page was detected on one of the JetBrains	2019-07-03	4.3	CVE-2019-12842

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TeamCity pages. The issue was fixed in TeamCity 2018.2.2.			CONFIRM
jetbrains -- teamcity	The generated Kotlin DSL settings allowed usage of an unencrypted connection for resolving artifacts. The issue was fixed in JetBrains TeamCity 2018.2.3.	2019-07-03	5.0	CVE-2019-12845 MISC
jetbrains -- teamcity	A user without the required permissions could gain access to some JetBrains TeamCity settings. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	4.0	CVE-2019-12846 CONFIRM
kubevirt -- containerized-data-importer	A flaw was found in the containerized-data-importer in virt-cdi-cloner, version 1.4, where the host-assisted cloning feature does not determine whether the requesting user has permission to access the Persistent Volume Claim (PVC) in the source namespace. This could allow users to clone any PVC in the cluster into their own namespace, effectively allowing access to other user's data.	2019-06-28	4.0	CVE-2019-10175 CONFIRM
lemonldap-ng -- lemonldap::	LemonLDAP::NG before 1.9.20 has an XML External Entity (XXE) issue when submitting a notification to the notification server. By default, the notification server is not enabled and has a "deny all" rule.	2019-06-28	6.8	CVE-2019-13031 MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mod_auth_mellon_project -- mod_auth_mellon	mod_auth_mellon through 0.14.2 has an Open Redirect via the login?ReturnTo= substring, as demonstrated by omitting the // after http: in the target URL.	2019-06-29	4.3	CVE-2019-13038 MISC
monstra -- monstra_cms	Monstra CMS before 3.0.4 has XSS via index.php.	2019-07-03	4.3	CVE-2018-11227 MISC MISC EXPLOIT-DB
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Cross-Site Request Forgery (CSRF).	2019-07-02	6.8	CVE-2019-7270 MISC MISC
nortekcontrol -- linear_emerge_5000p_firmware	Nortek Linear eMerge 50P/5000P devices have Default Credentials.	2019-07-01	5.0	CVE-2019-7271 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Default Credentials.	2019-07-02	5.0	CVE-2019-7252 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow XSS.	2019-07-02	4.3	CVE-2019-7255

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Privilege Escalation.	2019-07-02	6.5	CVE-2019-7258 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Authorization Bypass with Information Disclosure.	2019-07-02	4.0	CVE-2019-7259 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Cleartext Credentials in a Database.	2019-07-02	5.0	CVE-2019-7260 MISC MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Cross-Site Request Forgery (CSRF).	2019-07-02	6.8	CVE-2019-7262 MISC MISC
novaksolutions -- infusionsoft-php-sdk	novaksolutions/infusionsoft-php-sdk v2016-10-31 is vulnerable to a reflected XSS in the leadscoring.php resulting code execution	2019-07-03	4.3	CVE-2017-6216 MISC
odoo -- odoo	Improper data access control in Odoo Community 10.0 and 11.0	2019-07-03	4.0	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and Odoo Enterprise 10.0 and 11.0 allows authenticated users to perform a CSV export of the secure hashed passwords of other users.			14861 CONFIRM
odoo -- odoo	Incorrect access control in the mail templating system in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated internal users to delete arbitrary menuitems via a crafted RPC request.	2019-07-03	5.5	CVE-2018-14862 CONFIRM
odoo -- odoo	Incorrect access control in the RPC framework in Odoo Community 8.0 through 11.0 and Odoo Enterprise 9.0 through 11.0 allows authenticated users to call private functions via RPC.	2019-07-03	5.5	CVE-2018-14863 CONFIRM
odoo -- odoo	Incorrect access control in asset bundles in Odoo Community 9.0 through 11.0 and earlier and Odoo Enterprise 9.0 through 11.0 and earlier allows remote authenticated users to inject arbitrary web script via a crafted attachment.	2019-07-03	4.0	CVE-2018-14864 CONFIRM
odoo -- odoo	Report engine in Odoo Community 9.0 through 11.0 and earlier and Odoo Enterprise 9.0 through 11.0 and earlier does not use secure options when passing documents to wkhtmltopdf, which allows remote attackers to read local files.	2019-07-03	4.0	CVE-2018-14865 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
odoo -- odoo	Incorrect access control in the portal messaging system in Odoo Community 9.0 and 10.0 and Odoo Enterprise 9.0 and 10.0 allows remote attackers to post messages on behalf of customers, and to guess document attribute values, via crafted parameters.	2019-06-28	5.0	CVE-2018-14867 MISC CONFIRM
odoo -- odoo	Incorrect access control in the Password Encryption module in Odoo Community 9.0 and Odoo Enterprise 9.0 allows authenticated users to change the password of other users without knowing their current password via a crafted RPC call.	2019-06-28	4.0	CVE-2018-14868 MISC CONFIRM
odoo -- odoo	The module-description renderer in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier does not disable RST's local file inclusion, which allows privileged authenticated users to read local files via a crafted module description.	2019-06-28	4.0	CVE-2018-14886 MISC CONFIRM
odoo -- odoo	Improper Host header sanitization in the dbfilter routing component in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows a remote attacker to deny access to the service and to disclose database names via a crafted request.	2019-06-28	5.8	CVE-2018-14887 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-xchange -- ox_guard	OX Guard 2.8.0 has CSRF.	2019-07-03	6.8	CVE-2018-10986 CONFIRM
optergy -- enterprise	Optergy Proton/Enterprise devices allow Username Disclosure.	2019-07-01	5.0	CVE-2019-7272 BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Cross-Site Request Forgery (CSRF).	2019-07-01	6.8	CVE-2019-7273 BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Open Redirect.	2019-07-01	5.8	CVE-2019-7275 BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Unauthenticated Internal Network Information Disclosure.	2019-07-01	5.0	CVE-2019-7277 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
optergy -- enterprise	Optergy Proton/Enterprise devices have an Unauthenticated SMS Sending Service.	2019-07-01	6.4	CVE-2019-7278 BID MISC MISC
paloaltonetworks -- minemeld	Cross-site scripting vulnerability in Palo Alto Networks MineMeld version 0.9.60 and earlier may allow a remote attacker able to convince an authenticated MineMeld admin to type malicious input in the MineMeld UI could execute arbitrary JavaScript code in the admin?s browser.	2019-07-01	4.3	CVE-2019-1578 CONFIRM
paloaltonetworks -- traps	Code injection vulnerability in Palo Alto Networks Traps 5.0.5 and earlier may allow an authenticated attacker to inject arbitrary JavaScript or HTML.	2019-07-01	6.5	CVE-2019-1577 BID CONFIRM
primasystems -- flexair	Prima Systems FlexAir devices have an Insufficient Session-ID Length.	2019-07-01	4.0	CVE-2019-7280 MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices allow Cross-Site Request Forgery (CSRF).	2019-07-01	6.8	CVE-2019-7281 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
primasystems -- flexair	Prima Systems FlexAir devices allow authentication with MD5 hashes directly.	2019-07-01	6.5	CVE-2019-7666 MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices allow unauthenticated download of the database configuration backup due to a predictable name, resulting in authentication bypass (a login authenticated with the MD5 hash of any user found in the database).	2019-07-01	6.4	CVE-2019-7667 MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices have Default Credentials.	2019-07-01	5.0	CVE-2019-7668 MISC MISC
pulsesecure -- pulse_connect_secure	An XSS issue has been found with rd.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R3 due to improper header sanitization. This is not applicable to 8.1RX.	2019-06-28	4.3	CVE-2018-20808 CONFIRM
pulsesecure -- pulse_connect_secure	A crafted message can cause the web server to crash with Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R5 and Pulse Policy Secure 5.4RX before 5.4R5. This is not applicable to PCS 8.1RX.	2019-06-28	5.0	CVE-2018-20809 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pulsesecure -- pulse_connect_secure	A hidden RPC service issue was found with Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2 and 8.1RX before 8.1R12.	2019-06-28	5.0	CVE-2018-20811 CONFIRM
pulsesecure -- pulse_connect_secure	An XSS issue was found with Psaldownload.cgi in Pulse Secure Pulse Connect Secure (PCS) 8.3R2 before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX or PPS 5.2RX.	2019-06-28	4.3	CVE-2018-20814 BID CONFIRM
pulsesecure -- pulse_secure_desktop_client	An information exposure issue where IPv6 DNS traffic would be sent outside of the VPN tunnel (when Traffic Enforcement was enabled) exists in Pulse Secure Pulse Secure Desktop 9.0R1 and below. This is applicable only to dual-stack (IPv4/IPv6) endpoints.	2019-06-28	5.0	CVE-2018-20812 CONFIRM
rapid7 -- nexpose	A Cross-Site Request Forgery (CSRF) vulnerability was found in Rapid7 Nexpose InsightVM Security Console versions 6.5.0 through 6.5.68. This issue allows attackers to exploit CSRF vulnerabilities on API endpoints using Flash to circumvent a cross-domain pre-flight OPTIONS request.	2019-07-03	6.8	CVE-2019-5630 CONFIRM
redhat -- satellite	It was found that Spacewalk, all versions through 2.9, did not safely	2019-07-02	4.0	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	compute client token checksums. An attacker with a valid, but expired, authenticated set of headers could move some digits around, artificially extending the session validity without modifying the checksum.			10136 BID CONFIRM
rockoa -- rockoa	RockOA 1.8.7 allows remote attackers to obtain sensitive information because the webmain/webmainAction.php publictreestore method constructs a SQL WHERE clause unsafely by using the pidfields and idfields parameters, aka background SQL injection.	2019-06-28	4.0	CVE-2019-9846 MISC
seeddms -- seeddms	A stored XSS vulnerability was found in SeedDMS 5.1.11 due to poorly escaping the search result in the autocomplete search form placed in the header of out/out.Viewfolder.php.	2019-06-28	4.3	CVE-2019-12932 MISC
squirrelmail -- squirrelmail	XSS was discovered in SquirrelMail through 1.4.22 and 1.5.x through 1.5.2. Due to improper handling of RCDATA and RAWTEXT type elements, the built-in sanitization mechanism can be bypassed. Malicious script content from HTML e-mail can be executed within the application context via crafted use of (for example) a NOEMBED, NOFRAMES,	2019-07-01	4.3	CVE-2019-12970 MISC BUGTRAQ MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	NOSCRIPT, or TEXTAREA element.			
symantec -- endpoint_encryption	Symantec Endpoint Encryption, prior to SEE 11.3.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue that allows a user to gain elevated access to resources that are normally protected at lower access levels.	2019-07-01	4.6	CVE-2019-9702 BID CONFIRM
symantec -- endpoint_encryption	Symantec Endpoint Encryption, prior to SEE 11.3.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue that allows a user to gain elevated access to resources that are normally protected at lower access levels.	2019-07-01	4.6	CVE-2019-9703 BID CONFIRM
synology -- moments	Relative path traversal vulnerability in SYNO.PhotoTeam.Upload.Item in Synology Moments before 1.3.0-0691 allows remote authenticated users to upload arbitrary files via the name parameter.	2019-06-30	6.5	CVE-2019-11826 CONFIRM
synology -- photo_station	Relative path traversal vulnerability in SYNO.PhotoStation.File in Synology Photo Station before 6.8.11-3489 and before 6.3-2977 allows remote attackers to upload arbitrary files via the uploadphoto parameter.	2019-06-30	4.0	CVE-2019-11822 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable -- nessus	Content Injection vulnerability in Tenable Nessus prior to 8.5.0 may allow an authenticated, local attacker to exploit this vulnerability by convincing another targeted Nessus user to view a malicious URL and use Nessus to send fraudulent messages. Successful exploitation could allow the authenticated adversary to inject arbitrary text into the feed status, which will remain saved post session expiration.	2019-07-01	4.3	CVE-2019-3962 BID CONFIRM
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 allows a denial of service upon a critical error in certain sys_sbrk allocation patterns (involving PAGE_SIZE, and a value less than PAGE_SIZE).	2019-06-29	4.9	CVE-2019-13048 MISC
waspthemes -- custom_css_pro	Cross-site request forgery (CSRF) vulnerability in Custom CSS Pro 1.0.3 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5984 MISC MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000384e2a.	2019-06-30	6.8	CVE-2019-13083 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000026b739.	2019-06-30	6.8	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				13084 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000030ecfa.	2019-06-30	6.8	CVE-2019-13085 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000385474.	2019-07-04	6.8	CVE-2019-13253 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e808.	2019-07-04	6.8	CVE-2019-13254 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000327464.	2019-07-04	6.8	CVE-2019-13255 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e849.	2019-07-04	6.8	CVE-2019-13256 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x00000000003273aa.	2019-07-04	6.8	CVE-2019-13257 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000328165.	2019-07-04	6.8	CVE-2019-13258 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e566.	2019-07-04	6.8	CVE-2019-13259 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000327a07.	2019-07-04	6.8	CVE-2019-13260 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000328384.	2019-07-04	6.8	CVE-2019-13261 MISC
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x00000000003283eb.	2019-07-04	6.8	CVE-2019-13262 MISC
xpertsol -- server_status_by_hostname/ip	A SQL injection vulnerability in the Xpert Solution "Server Status by Hostname/IP" plugin 4.6 for WordPress allows an authenticated user to execute arbitrary SQL commands via GET parameters.	2019-07-03	6.5	CVE-2019-12570 MISC
zoneminder -- zoneminder	Stored XSS in the Filters page (Name field) in ZoneMinder 1.32.3 allows a malicious user to embed	2019-06-29	4.3	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and execute JavaScript code in the browser of any user who navigates to this page.			13072 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/page-edit.php (content box), which can be used to get a user's cookie.	2019-07-05	3.5	CVE-2019-13339 MISC
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the content box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, CVE-2018-20520, and CVE-2019-13186.	2019-07-05	3.5	CVE-2019-13340 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/conf.php (comment box), which can be used to get a user's cookie.	2019-07-05	3.5	CVE-2019-13341 MISC
f5 -- websafe_alert_server	Cross-Site-Scripting (XSS) vulnerabilities in F5 WebSafe Dashboard 3.9.5 and earlier, aka F5 WebSafe Alert Server, allow privileged authenticated users to inject arbitrary web script or HTML when creating a new user, account or signature.	2019-07-01	3.5	CVE-2016-5236 CONFIRM
fujielectric -- alpha7_pc_loader_firmware	An out-of-bounds read vulnerability has been identified in Fuji Electric Alpha7 PC Loader Versions 1.1 and prior, which may crash the system.	2019-07-02	3.3	CVE-2019-10975 BID MISC MISC
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, and 19.0.0.1 is vulnerable to cross-site scripting. This	2019-07-01	3.5	CVE-2019-4410 BID XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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: 162657.			
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.1, 10.5, and 11.1 is vulnerable to a denial of service. Users that have both EXECUTE on PD_GET_DIAG_HIST and access to the diagnostic directory on the DB2 server can cause the instance to crash. IBM X-Force ID: 158091.	2019-07-01	2.1	CVE-2019-4101 BID XF CONFIRM
ibm -- spectrum_protect	IBM Tivoli Storage Manager Server (IBM Spectrum Protect 7.1 and 8.1) could allow a local user to replace existing databases by restoring old data.	2019-07-02	3.6	CVE-2019-4140 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	IBM X-Force ID: 158336.			
synology -- calendar	Cross-site scripting (XSS) vulnerability in Event Editor in Synology Calendar before 2.3.0-0615 allows remote attackers to inject arbitrary web script or HTML via the title parameter.	2019-06-30	3.5	CVE-2019-11825 CONFIRM
synology -- note_station	Cross-site scripting (XSS) vulnerability in SYNO.NoteStation.Shard in Synology Note Station before 2.5.3-0863 allows remote attackers to inject arbitrary web script or HTML via the object_id parameter.	2019-06-30	3.5	CVE-2019-11827 CONFIRM
synology -- office	Cross-site scripting (XSS) vulnerability in Chart in Synology Office before 3.1.4-2771 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2019-06-30	3.5	CVE-2019-11828 CONFIRM

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a.t.works -- idoors_reader	iDoors Reader 2.10.17 and earlier allows an attacker on the same network segment to bypass authentication to access the management console and operate the product via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5964 MISC MISC
amcrest -- ipm-721s_devices	On Amcrest IPM-721S V2.420.AC00.16.R.20160909 devices, the users on the device are divided into 2 groups "admin" and "user". However, as a part of security analysis it was identified that a low privileged user who belongs to the "user" group and who has access to login in to the web administrative interface of the device can add a new administrative user to the interface using HTTP APIs provided by the device and perform all the actions as an administrative user by using that account. If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the	2019-07-03	not yet calculated	CVE-2017-8230 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable functions that performs the various action described in HTTP APIs. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function at address 0x00429084 in IDA pro is the one that processes the HTTP API request for "addUser" action. If one traces the calls to this function, it can be clearly seen that the function sub_41F38C at address 0x0041F588 parses the call received from the browser and passes it to the "addUser" function without any authorization check.			
amcrest -- ipm-721s_devices	The Amcrest IPM-721S Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322 allows HTTP requests that permit enabling various functionalities of the camera by using HTTP APIs, instead of the web management interface that is provided by the application. This HTTP	2019-07-03	not yet calculated	CVE-2017-13719 MISC MISC BUG

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	API receives the credentials as base64 encoded in the Authorization HTTP header. However, a missing length check in the code allows an attacker to send a string of 1024 characters in the password field, and allows an attacker to exploit a memory corruption issue. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials. If the firmware version Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322 is dissected using the binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that has many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the HTTP API specification. If we open this binary in IDA Pro we will notice that this follows an ARM little-endian format. The function at address 00415364 in IDA Pro starts the HTTP authentication process. This function calls			TRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	another function at sub_0042CCA0 at address 0041549C. This function performs a strchr operation after base64 decoding the credentials, and stores the result on the stack, which results in a stack-based buffer overflow.			
amcrest -- ipm-721s_devices	Amcrest IPM-721S V2.420.AC00.16.R.20160909 devices have default credentials that are hardcoded in the firmware and can be extracted by anyone who reverses the firmware to identify them. If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If one opens this binary in IDA-pro, one will notice that this follows a ARM little endian format. The function sub_3DB2FC in IDA pro is identified to be	2019-07-03	not yet calculated	CVE-2017-8226 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	setting up the values at address 0x003DB5A6. The sub_5C057C then sets this value and adds it to the Configuration files in /mnt/mtd/Config/Account1 file.			
amcrest -- ipm-721s_devices	Amcrest IPM-721S V2.420.AC00.16.R.20160909 devices have a timeout policy to wait for 5 minutes in case 30 incorrect password attempts are detected using the Web and HTTP API interface provided by the device. However, if the same brute force attempt is performed using the ONVIF specification (which is supported by the same binary) then there is no account lockout or timeout executed. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials. If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder.	2019-07-03	not yet calculated	CVE-2017-8227 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the ONVIF specification. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function at address 00671618 in IDA pro is parses the WSSE security token header. The sub_ 603D8 then performs the authentication check and if it is incorrect passes to the function sub_59F4C which prints the value "Sender not authorized."			
amcrest -- ipm-721s_devices	Amcrest IPM-721S V2.420.AC00.16.R.20160909 devices mishandle reboots within the past two hours. Amcrest cloud services does not perform a thorough verification when allowing the user to add a new camera to the user's account to ensure that the user actually owns the camera other than knowing the serial number of the camera. This can allow an attacker who knows the serial number to easily add another user's camera to an attacker's cloud account and control it completely. This is	2019-07-03	not yet calculated	CVE-2017-8228 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	possible in case of any camera that is currently not a part of an Amcrest cloud account or has been removed from the user's cloud account. Also, another requirement for a successful attack is that the user should have rebooted the camera in the last two hours. However, both of these conditions are very likely for new cameras that are sold over the Internet at many ecommerce websites or vendors that sell the Amcrest products. The successful attack results in an attacker being able to completely control the camera which includes being able to view and listen on what the camera can see, being able to change the motion detection settings and also be able to turn the camera off without the user being aware of it. Note: The same attack can be executed using the Amcrest Cloud mobile application.			
amcrest -- ipm-721s_devices	Amcrest IPM-721S V2.420.AC00.16.R.20160909 devices allow an unauthenticated attacker to download the administrative credentials. If the firmware	2019-07-03	not yet calculated	CVE-2017-8229 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function sub_436D6 in IDA pro is identified to be setting up the configuration for the device. If one scrolls to the address 0x000437C2 then one can see that /current_config is being set as an ALIAS for /mnt/mtd/Config folder on the device. If one TELNETs into the device and navigates to /mnt/mtd/Config folder, one can observe that it contains various files such as Account1, Account2, SHAACcount1, etc. This means that if one navigates to http://[IPofcamera]/current_config/Sha1Account1 then one should be able to view			CMISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the content of the files. The security researchers assumed that this was only possible only after authentication to the device. However, when unauthenticated access tests were performed for the same URL as provided above, it was observed that the device file could be downloaded without any authentication.			
arox -- school-erp_pro	AROX School-ERP Pro has a command execution vulnerability. import_stud.php and upload_fille.php do not have session control. Therefore an unauthenticated user can execute a command on the system.	2019-07-04	not yet calculated	CVE-2019-13294 MISC MISC
artica -- pandora_fms	Artica Pandora FMS 7.0 NG before 735 suffers from local privilege escalation due to improper permissions on C:\PandoraFMS and its sub-folders, allowing standard users to create new files. Moreover, the Apache service httpd.exe will try to execute cmd.exe from C:\PandoraFMS (the current directory) as NT AUTHORITY\SYSTEM upon web requests to the	2019-06-29	not yet calculated	CVE-2019-13035 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	portal. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM.			
artifex -- mupdf	Artifex MuPDF 1.15.0 has a heap-based buffer overflow in fz_append_display_node located at fitz/list-device.c, allowing remote attackers to execute arbitrary code via a crafted PDF file. This occurs with a large BDC property name that overflows the allocated size of a display list node.	2019-07-04	not yet calculated	CVE-2019-13290 MISC MISC MISC
axiosys -- bento4	An issue was discovered in Bento4 1.5.1.0. A memory allocation failure is unhandled in Core/Ap4SdpAtom.cpp and leads to crashes. When parsing input video, the program allocates a new buffer to parse an atom in the stream. The unhandled memory allocation failure causes a direct copy to a NULL pointer.	2019-07-04	not yet calculated	CVE-2019-13238 MISC
bks -- bks_ebk_ethernet_buskopple	BKS EBK Ethernet-Buskoppler Pro before 3.01	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
r_pro	allows Unrestricted Upload of a File with a Dangerous Type.	07-05	calculated	2019-12971 MISC
blipcare -- blipcare_wi-fi_blood_pressure_monitor	It was discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device allows to connect to web management interface on a non-SSL connection using plain text HTTP protocol. The user uses the web management interface of the device to provide the user's Wi-Fi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is connected to the Blipcare's device wireless network to easily sniff these values using a MITM attack.	2019-07-02	not yet calculated	CVE-2017-11578 MISC MISC BUGTRAQ
blipcare -- blipcare_wi-fi_blood_pressure_monitor	In the most recent firmware for Blipcare, the device provides an open Wireless network called "Blip" for communicating with the	2019-07-02	not yet calculated	CVE-2017-1157

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device. The user connects to this open Wireless network and uses the web management interface of the device to provide the user's Wi-Fi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is in vicinity of Wireless signal generated by the Blipcare device to easily sniff the credentials. Also, an attacker can connect to the open wireless network "Blip" exposed by the device and modify the HTTP response presented to the user by the device to execute other attacks such as convincing the user to download and execute a malicious binary that would infect a user's computer or mobile device with malware.			9 MISC MISC BUGTRAQ
blipcare -- blipcare_wi-fi_blood_pressure_monitor	Blipcare Wifi blood pressure monitor BP700 10.1 devices allow memory corruption that results in Denial of Service. When connected to the "Blip" open wireless connection provided by the	2019-07-02	not yet calculated	CVE-2017-11580 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device, if a large string is sent as a part of the HTTP request in any part of the HTTP headers, the device could become completely unresponsive. Presumably this happens as the memory footprint provided to this device is very small. According to the specs from Rezolt, the Wi-Fi module only has 256k of memory. As a result, an incorrect string copy operation using either memcpy, strcpy, or any of their other variants could result in filling up the memory space allocated to the function executing and this would result in memory corruption. To test the theory, one can modify the demo application provided by the Cypress WICED SDK and introduce an incorrect "memcpy" operation and use the compiled application on the evaluation board provided by Cypress semiconductors with exactly the same Wi-Fi SOC. The results were identical where the device would completely stop responding to any of the ping or web requests.			CMISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
blogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 allows /api/filemanager Directory Traversal via the path parameter.	2019-07-03	not yet calculated	CVE-2019-10717 FULLDISC MISC MISC
blogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 allows a Client Side URL Redirect via the ReturnUrl parameter, related to BlogEngine/BlogEngine.Core/Services/Security/Security.cs, login.aspx, and register.aspx.	2019-07-03	not yet calculated	CVE-2019-10721 MISC MISC
calamares -- calamares	Calamares versions 3.1 through 3.2.10 copies a LUKS encryption keyfile from /crypto_keyfile.bin (mode 0600 owned by root) to /boot within a globally readable initramfs image with insecure permissions, which allows this originally protected file to be read by any user, thereby disclosing decryption keys for LUKS	2019-07-02	not yet calculated	CVE-2019-13179 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	containers created with Full Disk Encryption.			MISC
calamares -- calamares	modules/luksbootkeyfile/main.py in Calamares versions 3.1 through 3.2.10 has a race condition between the time when the LUKS encryption keyfile is created and when secure permissions are set.	2019-07-02	not yet calculated	CVE-2019-13178 MISC MISC MISC MISC MISC MISC MISC
centreon -- centreon	Centreon V19.04 allows the attacker to execute arbitrary system commands by using the value "init_script"-"Monitoring Engine Binary" in main.get.php to insert a arbitrary command into the database, and execute it by calling the vulnerable page www/include/configuration/configGenerate/xml/generateFiles.php (which passes the inserted value to the database	2019-07-01	not yet calculated	CVE-2019-13024 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to shell_exec without sanitizing it, allowing one to execute system arbitrary commands).			
cisco -- 7800_and_8800_series_ip_phones	A vulnerability in Cisco SIP IP Phone Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected phone. The vulnerability is due to insufficient validation of input Session Initiation Protocol (SIP) packets. An attacker could exploit this vulnerability by altering the SIP replies that are sent to the affected phone during the registration process. A successful exploit could allow the attacker to cause the phone to reboot and not complete the registration process.	2019-07-05	not yet calculated	CVE-2019-1922 CISCO
cisco -- advanced_malware_protection_for_endpoints_for_windows	A vulnerability in Cisco Advanced Malware Protection (AMP) for Endpoints for Windows could allow an authenticated, local attacker with administrator privileges to execute arbitrary code. The vulnerability is due to	2019-07-05	not yet calculated	CVE-2019-1932 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	insufficient validation of dynamically loaded modules. An attacker could exploit this vulnerability by placing a file in a specific location in the Windows filesystem. A successful exploit could allow the attacker to execute the code with the privileges of the AMP service.			
cisco -- application_policy_infrastructure_controller_software	A vulnerability in the REST API for software device management in Cisco Application Policy Infrastructure Controller (APIC) Software could allow an authenticated, remote attacker to escalate privileges to root on an affected device. The vulnerability is due to incomplete validation and error checking for the file path when specific software is uploaded. An attacker could exploit this vulnerability by uploading malicious software using the REST API. A successful exploit could allow an attacker to escalate their privilege level to root. The attacker would need to have the administrator role on the device.	2019-07-04	not yet calculated	CVE-2019-1889 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- email_security_appliance	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device. The vulnerability is due to improper input validation of certain email fields. An attacker could exploit this vulnerability by sending a crafted email message to a recipient protected by the ESA. A successful exploit could allow the attacker to bypass configured message filters and inject arbitrary scripting code inside the email body. The malicious code is not executed by default unless the recipient's email client is configured to execute scripts contained in emails.	2019-07-05	not yet calculated	CVE-2019-1933 CISCO
cisco -- email_security_appliance	A vulnerability in the attachment scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper input validation of	2019-07-05	not yet calculated	CVE-2019-1921 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the email body. An attacker could exploit this vulnerability by naming a malicious attachment with a specific pattern. A successful exploit could allow the attacker to bypass configured content filters that would normally block the attachment.			
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker with administrator privileges to overwrite or read arbitrary files on the underlying operating system (OS) of an affected device. The vulnerability is due to improper input validation in NFVIS filesystem commands. An attacker could exploit this vulnerability by using crafted variables during the execution of an affected command. A successful exploit could allow the attacker to overwrite or read arbitrary files on the underlying OS.	2019-07-05	not yet calculated	CVE-2019-1894 CISCO
cisco -- enterprise_nfv_infrastructure	A vulnerability in Cisco Enterprise NFV	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_software	Infrastructure Software (NFVIS) could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device as root. The vulnerability is due to insufficient input validation of a configuration file that is accessible to a local shell user. An attacker could exploit this vulnerability by including malicious input during the execution of this file. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS as root.	07-05	calculated	2019-1893 CISCO
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected	2019-07-05	not yet calculated	CVE-2019-1931 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device. An attacker could exploit these vulnerabilities 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 -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities 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	2019-07-05	not yet calculated	CVE-2019-1930 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	interface or access sensitive, browser-based information.			
cisco -- ios_xr_software	A vulnerability in the implementation of Border Gateway Protocol (BGP) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to incorrect processing of certain BGP update messages. An attacker could exploit this vulnerability by sending BGP update messages that include a specific set of attributes to be processed by an affected system. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP traffic from explicitly defined peers only. To exploit this vulnerability, the malicious BGP update message would need to come from a configured, valid BGP peer or would need to be injected by the attacker into the victim's BGP	2019-07-05	not yet calculated	CVE-2019-1909 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	network on an existing, valid TCP connection to a BGP peer.			
cisco -- jabber	A vulnerability in the loading mechanism of specific dynamic link libraries in Cisco Jabber for Windows could allow an authenticated, local attacker to perform a DLL preloading attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of the resources loaded by the application at run time. An attacker could exploit this vulnerability by crafting a malicious DLL file and placing it in a specific location on the targeted system. The malicious DLL file would execute when the Jabber application launches. A successful exploit could allow the attacker to execute arbitrary code on the target machine with the privileges of another user's account.	2019-07-04	not yet calculated	CVE-2019-1855 BID CISCO
cisco -- nexus_9000_series_switches	A vulnerability in the fabric infrastructure VLAN connection establishment of the Cisco Nexus 9000 Series	2019-07-04	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, adjacent attacker to bypass security validations and connect an unauthorized server to the infrastructure VLAN. The vulnerability is due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. An attacker could exploit this vulnerability by sending a malicious LLDP packet on the adjacent subnet to the Cisco Nexus 9000 Series Switch in ACI mode. A successful exploit could allow the attacker to connect an unauthorized server to the infrastructure VLAN, which is highly privileged. With a connection to the infrastructure VLAN, the attacker can make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints.		ulated	1890 BID CISCO
cisco -- small_business_200_and_300_and_500_series_managed_	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500	2019-	not yet calc	CVE-2019

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
switches	Series Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	07-05	ulated	-1891 CISCO
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the Secure Sockets Layer (SSL) input packet processor of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a memory corruption on an affected device. The vulnerability is due to improper validation of HTTPS packets. An attacker could exploit this vulnerability by sending a malformed HTTPS packet to the management web interface of the affected	2019-07-05	not yet calculated	CVE-2019-1892 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a denial of service (DoS) condition.			
cisco -- unified_communications_domain_manager	A vulnerability in the CLI of Cisco Unified Communications Domain Manager (Cisco Unified CDM) Software could allow an authenticated, local attacker to escape the restricted shell. The vulnerability is due to insufficient input validation of shell commands. An attacker could exploit this vulnerability by executing crafted commands in the shell. A successful exploit could allow the attacker to escape the restricted shell and access commands in the context of the restricted shell user, which does not have root privileges.	2019-07-05	not yet calculated	CVE-2019-1911 CISCO
cisco -- unified_communications_manager	A vulnerability in the Session Initiation Protocol (SIP) protocol implementation of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to cause a denial of	2019-07-05	not yet calculated	CVE-2019-1887 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	service (DoS) condition. The vulnerability is due to insufficient validation of input SIP traffic. An attacker could exploit this vulnerability by sending a malformed SIP packet to an affected Cisco Unified Communications Manager. A successful exploit could allow the attacker to trigger a new registration process on all connected phones, temporarily disrupting service.			
cisco -- web_security_appliance	A vulnerability in the HTTPS decryption feature of Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Secure Sockets Layer (SSL) server certificates. An attacker could exploit this vulnerability by installing a malformed certificate in a web server and sending a request to it through the Cisco WSA. A successful exploit could allow the attacker to cause an unexpected restart of the	2019-07-04	not yet calculated	CVE-2019-1886 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	proxy process on an affected device.			
cisco -- web_security_appliance	A vulnerability in the web proxy functionality of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation mechanisms for certain fields in HTTP/HTTPS requests sent through an affected device. A successful attacker could exploit this vulnerability by sending a malicious HTTP/HTTPS request through an affected device. An exploit could allow the attacker to force the device to stop processing traffic, resulting in a DoS condition.	2019-07-04	not yet calculated	CVE-2019-1884 CISCO
cloudera -- cloudera_manager	The keystore password for the Spark History Server may be exposed in unsecured files under the /var/run/cloudera-scm-agent directory managed by Cloudera Manager. The keystore file itself is not exposed.	2019-07-03	not yet calculated	CVE-2017-9326 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cloudera -- cloudera_manager	Secret data of processes managed by CM is not secured by file permissions.	2019-07-03	not yet calculated	CVE-2017-9327 CONFIRM
cloudera -- data_science_workbench	Remote code execution is possible in Cloudera Data Science Workbench version 1.3.0 and prior releases via unspecified attack vectors.	2019-07-03	not yet calculated	CVE-2018-11215 CONFIRM
cloudera -- solr	The provided secure solrconfig.xml sample configuration does not enforce Sentry authorization on /update/json/docs.	2019-07-03	not yet calculated	CVE-2017-9325 CONFIRM
codedoc -- codedoc	Codedoc v3.2 has a stack-based buffer overflow in add_variable in codedoc.c, related to codedoc_strlcpy.	2019-07-06	not yet calculated	CVE-2019-13362 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeigniter-restserver -- codeigniter-restserver	CodeIgniter Rest Server (aka codeigniter-restserver) 2.7.1 allows XXE attacks.	2019-07-03	not yet calculated	CVE-2015-3907 MISC
curl -- curl	A non-privileged user or program can put code and a config file in a known non-privileged path (under C:/usr/local/) that will make curl <= 7.65.1 automatically run the code (as an openssl "engine") on invocation. If that curl is invoked by a privileged user it can do anything it wants.	2019-07-02	not yet calculated	CVE-2019-5443 MLIST BID MISC
d-link -- central_wifi_manager	An issue was discovered in the D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6. Input does not get validated and arbitrary SQL statements can be executed in the database via the /web/Public/Conn.php parameter dbSQL.	2019-07-06	not yet calculated	CVE-2019-13373 MISC MISC
d-link -- central_wifi_manager	A cross-site scripting (XSS) vulnerability in resource view in PayAction.class.php in D-Link Central WiFi Manager CWM(100) before	2019-07-06	not yet calculated	CVE-2019-1337

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	v1.03R0100_BETA6 allows remote attackers to inject arbitrary web script or HTML via the index.php/Pay/passcodeAuth passcode parameter.			4 MISC MISC
d-link -- central_wifi_manager	A SQL Injection was discovered in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 in PayAction.class.php with the index.php/Pay/passcodeAuth parameter passcode. The vulnerability does not need any authentication.	2019-07-06	not yet calculated	CVE-2019-13375 MISC MISC
d-link -- central_wifi_manager	/web/Lib/Action/IndexAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to execute arbitrary PHP code via a cookie because a cookie's username field allows eval injection, and an empty password bypasses authentication.	2019-07-06	not yet calculated	CVE-2019-13372 MISC MISC
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The binary orthrus in /sbin folder of the device handles all the UPnP	2019-07-02	not yet calculated	CVE-2017-8414

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	connections received by the device. It seems that the binary performs a sprintf operation at address 0x0000A3E4 with the value in the command line parameter "-f" and stores it on the stack. Since there is no length check, this results in corrupting the registers for the function sub_A098 which results in memory corruption.			MISC MISC BUGTRAQ
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1130 and DCS-1100 devices. The binary rtspd in /sbin folder of the device handles all the rtsp connections received by the device. It seems that the binary loads at address 0x00012CF4 a flag called "Authenticate" that indicates whether a user should be authenticated or not before allowing access to the video feed. By default, the value for this flag is zero and can be set/unset using the HTTP interface and network settings tab as shown below. The device requires that a user logging to the HTTP management interface of the device to provide a valid username and password.	2019-07-02	not yet calculated	CVE-2017-8405 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	However, the device does not enforce the same restriction by default on RTSP URL due to the checkbox unchecked by default, thereby allowing any attacker in possession of external IP address of the camera to view the live video feed. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.			
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The binary rtspd in /sbin folder of the device handles all the rtsp connections received by the device. It seems that the binary performs a memcpy operation at address 0x00011E34 with the value sent in the "Authorization: Basic" RTSP header and stores it on the stack. The number of bytes to be copied are calculated based on the length of the string sent in the RTSP header by the client. As a result, memcpy copies more data then it can hold on stack and this results in corrupting the registers for the caller function sub_F6CC which results in memory	2019-07-02	not yet calculated	CVE-2017-8410 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	corruption. The severity of this attack is enlarged by the fact that the same value is then copied on the stack in the function 0x00011378 and this allows to overflow the buffer allocated and thus control the PC register which will result in arbitrary code execution on the device.			
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device has a custom binary called mp4ts under the /var/www/video folder. It seems that this binary dumps the HTTP VERB in the system logs. As a part of doing that it retrieves the HTTP VERB sent by the user and uses a vulnerable sprintf function at address 0x0000C3D4 in the function sub_C210 to copy the value into a string and then into a log file. Since there is no bounds check being performed on the environment variable at address 0x0000C360 this results in a stack overflow and overwrites the PC register allowing an attacker to execute buffer overflow or even a command injection attack.	2019-07-02	not yet calculated	CVE-2017-8412 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device runs a custom daemon on UDP port 5978 which is called "dldps2121" and listens for broadcast packets sent on 255.255.255.255. This daemon handles custom D-Link UDP based protocol that allows D-Link mobile applications and desktop applications to discover D-Link devices on the local network. The binary processes the received UDP packets sent from any device in "main" function. One path in the function traverses towards a block of code that handles commands to be executed on the device. The custom protocol created by D-Link follows the following pattern: Packetlen, Type of packet; M=MAC address of device or broadcast; D=Device Type;C=base64 encoded command string;test=1111. If a packet is received with the packet type being "S" or 0x53 then the string passed in the "C" parameter is base64 decoded and then executed by passing into a System API. We can see at address 0x00009B44 that the string received in	2019-07-02	not yet calculated	CVE-2017-8413 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	packet type subtracts 0x31 or "1" from the packet type and is compared against 0x22 or "double quotes". If that is the case, then the packet is sent towards the block of code that executes a command. Then the value stored in "C" parameter is extracted at address 0x0000A1B0. Finally, the string received is base 64 decoded and passed on to the system API at address 0x0000A2A8 as shown below. The same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third-party application on the device to execute commands on the device without any authentication by sending just 1 UDP packet with custom base64 encoding.			
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device has a custom telnet daemon as a part of the busybox and retrieves the password from the shadow file using the function getspnam at address 0x00053894. Then performs a crypt operation on the	2019-07-02	not yet calculated	CVE-2017-8415 MISC MISC BUG

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	password retrieved from the user at address 0x000538E0 and performs a strcmp at address 0x00053908 to check if the password is correct or incorrect. However, the /etc/shadow file is a part of CRAM-FS filesystem which means that the user cannot change the password and hence a hardcoded hash in /etc/shadow is used to match the credentials provided by the user. This is a salted hash of the string "admin" and hence it acts as a password to the device which cannot be changed as the whole filesystem is read only.			TRAQ
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device runs a custom daemon on UDP port 5978 which is called "dldps2121" and listens for broadcast packets sent on 255.255.255.255. This daemon handles custom D-Link UDP based protocol that allows D-Link mobile applications and desktop applications to discover D-Link devices on the local network. The binary processes the received UDP	2019-07-02	not yet calculated	CVE-2017-8416 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	packets sent from any device in "main" function. One path in the function traverses towards a block of code that processing of packets which does an unbounded copy operation which allows to overflow the buffer. The custom protocol created by Dlink follows the following pattern: Packetlen, Type of packet; M=MAC address of device or broadcast; D=Device Type;C=base64 encoded command string;test=1111 We can see at address function starting at address 0x0000DBF8 handles the entire UDP packet and performs an insecure copy using strcpy function at address 0x0000DC88. This results in overflowing the stack pointer after 1060 characters and thus allows to control the PC register and results in code execution. The same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third-party application on the device to execute commands on the device without any authentication by sending			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	just 1 UDP packet with custom base64 encoding.			
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device requires that a user logging into the device provide a username and password. However, the device allows D-Link apps on the mobile devices and desktop to communicate with the device without any authentication. As a part of that communication, the device uses custom version of base64 encoding to pass data back and forth between the apps and the device. However, the same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third party to retrieve the device's password without any authentication by sending just 1 UDP packet with custom base64 encoding. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.	2019-07-02	not yet calculated	CVE-2017-8417 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device requires that a user logging to the device to provide a username and password. However, the device does not enforce the same restriction on a specific URL thereby allowing any attacker in possession of that to view the live video feed. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.	2019-07-02	not yet calculated	CVE-2017-8409 MISC MISC BUGTRAQ
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder for the video clippings recorded by the device. It seems that the POST parameters passed in this request (to test if email credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the function and thus result in command injection on the device. If the firmware version is dissected using binwalk tool, we obtain a cramfs-root archive which contains the filesystem set up on the	2019-07-02	not yet calculated	CVE-2017-8411 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device that contains all the binaries. The library "libmailutils.so" is the one that has the vulnerable function "sub_1FC4" that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows an ARM little endian format. The function sub_1FC4 in IDA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "receiver1" is extracted in function "sub_15AC" which is then passed to the vulnerable system API call. The vulnerable library function is accessed in "cgibox" binary at address 0x00023BCC which calls the "Send_mail" function in "libmailutils.so" binary as shown below which results in the vulnerable POST parameter being passed to the library which results in the command injection issue.			
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder for the video clippings recorded by the	2019-07-02	not yet calculated	CVE-2017-8408 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device. It seems that the GET parameters passed in this request (to test if SMB credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the function and thus result in command injection on the device. If the firmware version is dissected using binwalk tool, we obtain a cramfs-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "cgibox" is the one that has the vulnerable function "sub_7EAFC" that receives the values sent by the GET request. If we open this binary in IDA-pro we will notice that this follows a ARM little endian format. The function sub_7EAFC in IDA pro is identified to be receiving the values sent in the GET request and the value set in GET parameter "user" is extracted in function sub_7E49C which is then passed to the vulnerable system API call.			C BUG TRA Q
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices.	2019-	not yet	CVE -

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The device provides a user with the capability of changing the administrative password for the web management interface. It seems that the device does not implement any cross-site request forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface to change the user's password.	07-02	calculated	2017-8407 MISC MISC BUGTRAQ
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a crossdomain.xml file with no restrictions on who can access the webserver. This allows an hosted flash file on any domain to make calls to the device's webserver and pull any information that is stored on the device. In this case, user's credentials are stored in clear text on the device and can be pulled easily. It also seems that the device does not implement any cross-site scripting forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a cross-site	2019-07-02	not yet calculated	CVE-2017-8406 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	flashing attack on the user's browser and execute any action on the device provided by the web management interface which steals the credentials from tools_admin.cgi file's response and displays it inside a Textfield.			
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder for the video clippings recorded by the device. It seems that the POST parameters passed in this request (to test if email credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the function and thus result in command injection on the device. If the firmware version is dissected using binwalk tool, we obtain a cramfs-root archive which contains the filesystem set up on the device that contains all the binaries. The library "libmailutils.so" is the one that has the vulnerable function "sub_1FC4" that receives the values sent by	2019-07-02	not yet calculated	CVE-2017-8404 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the POST request. If we open this binary in IDA-pro we will notice that this follows an ARM little endian format. The function sub_1FC4 in IDA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "receiver1" is extracted in function "sub_15AC" which is then passed to the vulnerable system API call. The vulnerable library function is accessed in "cgibox" binary at address 0x0008F598 which calls the "mailLoginTest" function in "libmailutils.so" binary as shown below which results in the vulnerable POST parameter being passed to the library which results in the command injection issue.			
d-link -- dir-823g_devices	An issue was discovered on D-Link DIR-823G devices with firmware 1.02B03. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the IPAddress or Gateway field to SetStaticRouteSettings.	2019-07-01	not yet calculated	CVE-2019-13128 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
diffplug -- spotless	In DiffPlug Spotless before 1.20.0 (library and Maven plugin) and before 3.20.0 (Gradle plugin), the XML parser would resolve external entities over both HTTP and HTTPS and didn't respect the resolveExternalEntities setting. For example, this allows disclosure of file contents to a MITM attacker if a victim performs a spotlessApply operation on an untrusted XML file.	2019-06-28	not yet calculated	CVE-2019-9843 MISC MISC MISC MISC
digisol -- dg-hr3400_wireless_broadband_home_router	DIGISOL DG-HR3400 devices have XSS via a modified SSID when the apssid value is unchanged.	2019-07-03	not yet calculated	CVE-2018-12715 MISC EXPLOIT-DB
digisol -- hr-3300_wireless_wifi_home_router	Digisol Wireless Wifi Home Router HR-3300 allows XSS via the userid or password parameter to the admin login page.	2019-07-05	not yet calculated	CVE-2018-14027 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
django -- django	An issue was discovered in Django 1.11 before 1.11.22, 2.1 before 2.1.10, and 2.2 before 2.2.3. An HTTP request is not redirected to HTTPS when the SECURE_PROXY_SSL_HEADER and SECURE_SSL_REDIRECT settings are used, and the proxy connects to Django via HTTPS. In other words, django.http.HttpRequest.scheme has incorrect behavior when a client uses HTTP.	2019-07-01	not yet calculated	CVE-2019-12781 MLIST BID MISC MISC CONFIRM UBUNTU DEBIAN CONFIRM
django_rest_registration -- django_rest_registration	verification.py in django-rest-registration (aka Django REST Registration library) before 0.5.0 relies on a static string for signatures (i.e., the Django Signing API is misused), which allows remote attackers to spoof the verification process. This occurs because incorrect code refactoring led to calling a security-critical	2019-07-02	not yet calculated	CVE-2019-13177 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	function with an incorrect argument.			
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.2 incorrectly converts encryption key source values, resulting in lower than expected entropy. NOTE: this issue exists because of an incomplete fix for CVE-2018-15812.	2019-07-03	not yet calculated	CVE-2018-18326 MISC MISC
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.2 uses a weak encryption algorithm to protect input parameters. NOTE: this issue exists because of an incomplete fix for CVE-2018-15811.	2019-07-03	not yet calculated	CVE-2018-18325 MISC MISC
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.1 incorrectly converts encryption key source values, resulting in lower than expected entropy.	2019-07-03	not yet calculated	CVE-2018-15812 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.1 uses a weak encryption algorithm to protect input parameters.	2019-07-03	not yet calculated	CVE-2018-15811 MISC MISC
dosbox -- dosbox	A buffer overflow in DOSBox 0.74-2 allows attackers to execute arbitrary code.	2019-07-03	not yet calculated	CVE-2019-7165 MLIST FEDORA MISC CONFIRM
eventum -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/switch.php has an Open Redirect via the current_page parameter.	2019-07-05	not yet calculated	eve
f5 -- big-ip	In BIG-IP 15.0.0, 14.0.0-14.1.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.2, and 11.5.2-11.6.4, BIG-IQ 6.0.0-6.1.0	2019-07-01	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and 5.1.0-5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, authenticated users with the ability to upload files (via scp, for example) can escalate their privileges to allow root shell access from within the TMOS Shell (tmsh) interface. The tmsh interface allows users to execute a secondary program via tools like sftp or scp.		ulated	6642 CONFIRM
f5 -- big-ip	On BIG-IP 12.1.0-12.1.4.1, undisclosed requests can cause iControl REST processes to crash. The attack can only come from an authenticated user; all roles are capable of performing the attack. Unauthenticated users cannot perform this attack.	2019-07-03	not yet calculated	CVE-2019-6641 CONFIRM
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, SNMP exposes sensitive configuration objects over insecure transmission channels. This issue is exposed when a passphrase is inserted into various profile types and accessed using SNMPv2.	2019-07-03	not yet calculated	CVE-2019-6640 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip	On BIG-IP (AFM, PEM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, an undisclosed TMUI pages for AFM and PEM Subscriber management are vulnerable to a stored cross-site scripting (XSS) issue. This is a control plane issue only and is not accessible from the data plane. The attack requires a malicious resource administrator to store the XSS.	2019-07-03	not yet calculated	CVE-2019-6639 CONFIRM
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, Malformed http requests made to an undisclosed iControl REST endpoint can lead to infinite loop of the restjavad process.	2019-07-03	not yet calculated	CVE-2019-6638 CONFIRM
f5 -- big-ip	On BIG-IP (ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, Application logic abuse of ASM REST endpoints can lead to instability of BIG-IP system. Exploitation of this issue causes excessive memory consumption which results in the Linux kernel triggering	2019-07-03	not yet calculated	CVE-2019-6637 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	OOM killer on arbitrary processes. The attack requires an authenticated user with role of "Guest" or greater privilege. Note: "No Access" cannot login so technically it's a role but a user with this access role cannot perform the attack.			
f5 -- big-ip	On BIG-IP (AFM, ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, and 11.5.1-11.6.4, a stored cross-site scripting vulnerability in AFM feed list. In the worst case, an attacker can store a CSRF which results in code execution as the admin user. The level of user role which can perform this attack are resource administrator and administrator.	2019-07-03	not yet calculated	CVE-2019-6636 CONFIRM
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, when the BIG-IP system is licensed for Appliance mode, a user with either the Administrator or the Resource Administrator role can bypass Appliance mode restrictions.	2019-07-03	not yet calculated	CVE-2019-6635 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, a high volume of malformed analytics report requests leads to instability in restjavad process. This causes issues with both iControl REST and some portions of TMUI. The attack requires an authenticated user with any role.	2019-07-03	not yet calculated	CVE-2019-6634 CONFIRM
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4, when the BIG-IP system is licensed with Appliance mode, user accounts with Administrator and Resource Administrator roles can bypass Appliance mode restrictions.	2019-07-03	not yet calculated	CVE-2019-6633 CONFIRM
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, under certain circumstances, attackers can decrypt configuration items that are encrypted because the vCMP configuration unit key is generated with insufficient randomness. The attack prerequisite is direct access	2019-07-03	not yet calculated	CVE-2019-6632 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to encrypted configuration and/or UCS files.			
f5 -- big-ip	On BIG-IP 11.5.1-11.6.4, iRules performing HTTP header manipulation may cause an interruption to service when processing traffic handled by a Virtual Server with an associated HTTP profile, in specific circumstances, when the requests do not strictly conform to RFCs.	2019-07-03	not yet calculated	CVE-2019-6631 CONFIRM
f5 -- big-ip	On BIG-IP PEM 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, under certain conditions, the TMM process may terminate and restart while processing BIG-IP PEM traffic with the OpenVPN classifier.	2019-07-03	not yet calculated	CVE-2019-6628 CONFIRM
f5 -- big-ip	On BIG-IP (AFM, Analytics, ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, and 11.5.1-11.6.3.4, A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the Configuration utility.	2019-07-03	not yet calculated	CVE-2019-6626 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, and 11.5.1-11.6.4, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI) also known as the BIG-IP Configuration utility.	2019-07-03	not yet calculated	CVE-2019-6625 CONFIRM
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, undisclosed SSL traffic to a virtual server configured with a Client SSL profile may cause TMM to fail and restart. The Client SSL profile must have session tickets enabled and use DHE cipher suites to be affected. This only impacts the data plane, there is no impact to the control plane.	2019-07-03	not yet calculated	CVE-2019-6629 CONFIRM
f5 -- f5_ssl_orchestrator	On F5 SSL Orchestrator 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, undisclosed traffic flow may cause TMM to restart under certain circumstances.	2019-07-03	not yet calculated	CVE-2019-6630 CONFIRM
f5 -- f5_ssl_orchestrator	On F5 SSL Orchestrator 14.1.0-14.1.0.5, on rare	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	occasions, specific to a certain race condition, TMM may restart when SSL Forward Proxy enforces the bypass action for an SSL Orchestrator transparent virtual server with SNAT enabled.	07-03	calculated	2019-6627 CONFIRM
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x00000000001a95b1.	2019-07-04	not yet calculated	CVE-2019-13245 MISC
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x00000000000002d7d.	2019-07-04	not yet calculated	CVE-2019-13244 MISC
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x00000000001a9601.	2019-07-04	not yet calculated	CVE-2019-13246 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ffmpeg -- ffmpeg	block_cmp() in libavcodec/zmbvenc.c in FFmpeg 4.1.3 has a heap-based buffer over-read.	2019-07-04	not yet calculated	CVE-2019-13312 MISC
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349197 and 12.0-RELEASE before 12.0-RELEASE-p6, a bug in the non-default RACK TCP stack can allow an attacker to cause several linked lists to grow unbounded and cause an expensive list traversal on every packet being processed, leading to resource exhaustion and a denial of service.	2019-07-02	not yet calculated	CVE-2019-5599 MISC MISC MLIST MISC MISC BUGTRAQ FREEBSD MISC MISC CERT-VN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349622, 12.0-RELEASE before 12.0-RELEASE-p7, 11.3-PRERELEASE before r349624, 11.3-RC3 before 11.3-RC3-p1, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in iconv implementation may allow an attacker to write past the end of an output buffer. Depending on the implementation, an attacker may be able to create a denial of service, provoke incorrect program behavior, or induce a remote code execution.	2019-07-03	not yet calculated	CVE-2019-5600 MISC FREEBSD
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349628, 12.0-RELEASE before 12.0-RELEASE-p7, 11.3-PRERELEASE before r349629, 11.3-RC3 before 11.3-RC3-p1, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in the cdrom driver allows users with read access to the cdrom device to arbitrarily overwrite kernel memory when media is present thereby allowing a malicious user in the operator group to gain root privileges.	2019-07-03	not yet calculated	CVE-2019-5602 MISC FREEBSD

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r347474, 12.0-RELEASE before 12.0-RELEASE-p7, 11.2-STABLE before r347475, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in the FFS implementation causes up to three bytes of kernel stack memory to be written to disk as uninitialized directory entry padding.	2019-07-03	not yet calculated	CVE-2019-5601 MISC FREEBSD
glpi_project -- glpi	inc/user.class.php in GLPI before 9.4.3 allows XSS via a user picture.	2019-07-04	not yet calculated	CVE-2019-13239 MISC MISC MISC
gnome -- libxslt	In numbers.c in libxslt 1.1.33, a type holding grouping characters of an xsl:number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.	2019-06-30	not yet calculated	CVE-2019-13118 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
gnome -- libxslt	In numbers.c in libxslt 1.1.33, an xsl:number with certain format strings could lead to a uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, I, i, or 0, or any other character.	2019-06-30	not yet calculated	CVE-2019-13117 MISC MISC MISC
grouptime -- teamwire_desktop_client	Grouptime Teamwire Desktop Client 1.5.1 prior to 1.9.0 on Windows allows code injection via a template, leading to remote code execution. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	CVE-2018-17170 MISC
grouptime -- teamwire_desktop_client	The admin interface of the Grouptime Teamwire Client 1.5.1 prior to 1.9.0 on-premises messenger server allows stored XSS. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	CVE-2018-17560 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hawt -- hawtio	Hawt Hawtio through 2.5.0 is vulnerable to SSRF, allowing a remote attacker to trigger an HTTP request from an affected server to an arbitrary host via the initial /proxy/ substring of a URI.	2019-07-03	not yet calculated	CVE-2019-9827 MISC
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 could allow an authenticated user to execute a function that would cause the server to crash. IBM X-Force ID: 162714.	2019-07-01	not yet calculated	CVE-2019-4386 BID XF CONFIRM
ibm -- infosphere_information_server	A Cross-Frame Scripting vulnerability in IBM InfoSphere Information Server 11.3, 11.5, and 11.7 can allow an attacker to load the vulnerable application inside an HTML iframe tag on a malicious page. IBM X-Force ID: 159419.	2019-07-01	not yet calculated	CVE-2019-4237 XF CONFIRM
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow an attacker to obtain sensitive information due to missing authentication in Ignite	2019-07-01	not yet calculated	CVE-2019-4337 CONFIR

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	nodes. IBM X-Force ID: 161412.			M XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 161411.	2019-07-01	not yet calculated	CVE-2019-4336 CONFIRM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow a local user to obtain highly sensitive information from log files when debugging is enabled. IBM X-Force ID: 160765.	2019-07-01	not yet calculated	CVE-2019-4299 CONFIRM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 uses a high privileged PostgreSQL account for database access which could allow a local user to perform actions they should not have privileges to execute. IBM X-Force ID: 160764.	2019-07-01	not yet calculated	CVE-2019-4298 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow a remote authenticated attacker to conduct an LDAP injection. By using a specially crafted request, an attacker could exploit this vulnerability to make unauthorized queries or modify the LDAP content. IBM X-Force ID: 160761.	2019-07-01	not yet calculated	CVE-2019-4297 CONFIRM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 information disclosure could allow a local user to obtain e-mail contents from the client debug log file. IBM X-Force ID: 160759.	2019-07-01	not yet calculated	CVE-2019-4296 CONFIRM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow an attacker with specialized access to obtain highly sensitive from the credential vault. IBM X-Force ID: 160758.	2019-07-01	not yet calculated	CVE-2019-4295 CONFIRM XF
ibm -- spectrum_protect_plus	When using IBM Spectrum Protect Plus 10.1.0, 10.1.2, and 10.1.3 to protect Oracle	2019-	not yet calc	CVE-2019

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	or MongoDB databases, a redirected restore operation may result in an escalation of user privileges. IBM X-Force ID: 162165.	07-01	ulated	- 4383 CONFIRM BID XF
ibm -- spectrum_protect_plus	When using IBM Spectrum Protect Plus 10.1.0, 10.1.2, and 10.1.3 to protect Oracle, DB2 or MongoDB databases, a redirected restore operation specifying a target path may allow execution of arbitrary code on the system. IBM X-Force ID: 161667,	2019-07-01	not yet calculated	CVE-2019-4357 CONFIRM BID XF
ibm -- spectrum_protect_servers	IBM Spectrum Protect Operations Center 7.1 and 8.1 could allow a remote attacker to obtain sensitive information, caused by an error message containing a stack trace. By creating an error with a stack trace, an attacker could exploit this vulnerability to potentially obtain details on the Operations Center architecture. IBM X-Force ID: 158279.	2019-07-02	not yet calculated	CVE-2019-4129 CONFIRM XF
ibm -- spectrum_protect_servers_an	IBM Spectrum Protect Servers 7.1 and 8.1 and	2019-	not yet	CVE -

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d_storage_agents	Storage Agents are vulnerable to a stack-based buffer overflow, caused by improper bounds checking by servers and storage agents in response to specifically crafted communication exchanges. By sending an overly long request, a remote attacker could overflow a buffer and execute arbitrary code on the system with instance id privileges or cause the server or storage agent to crash. IBM X-Force ID: 157510.	07-02	calculated	2019-4087 CONFIRM XF
ibm -- spectrum_protect_servers_and_storage_agents	IBM Spectrum Protect Servers 7.1 and 8.1 and Storage Agents could allow a local attacker to gain elevated privileges on the system, caused by loading a specially crafted library loaded by the dsmqsan module. By setting up such a library, a local attacker could exploit this vulnerability to gain root privileges on the vulnerable system. IBM X-Force ID: 157511.	2019-07-02	not yet calculated	CVE-2019-4088 CONFIRM XF
ignited_cms -- ignited_cms	index.php/admin/permissions in Ignited CMS through 2017-02-19 allows CSRF to add an administrator.	2019-07-06	not yet calculated	CVE-2019-1337

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				0 MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/fourier.c in ComplexImages.	2019-07-04	not yet calculated	CVE-2019-13302 MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of off-by-one errors.	2019-07-04	not yet calculated	CVE-2019-13306 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of a wand/mogrify.c error.	2019-07-04	not yet calculated	CVE-2019-13311 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling rows.	2019-07-04	not yet calculated	CVE-2019-13307 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced strncpy and an off-by-one error.	2019-07-04	not yet calculated	CVE-2019-13305 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced assignment.	2019-07-04	not yet calculated	CVE-2019-1330

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				4 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/composite.c in CompositeImage.	2019-07-04	not yet calculated	CVE-2019-13303 MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks in AcquireMagickMemory because of an AnnotateImage error.	2019-07-04	not yet calculated	CVE-2019-13301 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in	2019-07-04	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	EvaluateImages because of mishandling columns.		ulated	13300 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/pixel-accessor.h in GetPixelChannel.	2019-07-04	not yet calculated	CVE-2019-13299 MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/pixel-accessor.h in SetPixelViaPixelInfo because of a MagickCore/enhance.c error.	2019-07-04	not yet calculated	CVE-2019-13298 MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage	2019-07-04	not yet calculated	CVE-2019-1329

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	because a height of zero is mishandled.			7 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has direct memory leaks in AcquireMagickMemory because of an error in CLIListOperatorImages in MagickWand/operation.c for a NULL value.	2019-07-04	not yet calculated	CVE-2019-13296 MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a width of zero is mishandled.	2019-07-04	not yet calculated	CVE-2019-13295 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow in	2019-07-04	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	MagickCore/fourier.c in ComplexImage.		ulated	13308 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of mishandling the NoSuchImage error in CLIListOperatorImages in MagickWand/operation.c.	2019-07-04	not yet calculated	CVE-2019-13309 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of an error in MagickWand/mogrify.c.	2019-07-04	not yet calculated	CVE-2019-13310 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
invoxia -- nvx220_devices	Invoxia NVX220 devices allow access to /bin/sh via escape from a restricted CLI, leading to disclosure of password hashes.	2019-07-05	not yet calculated	CVE-2018-14529 MISC
invoxia -- nvx220_devices	Invoxia NVX220 devices allow TELNET access as admin with a default password.	2019-07-05	not yet calculated	CVE-2018-14528 MISC
irfanview -- irfanview	IrfanView 4.52 has a User Mode Write AV starting at image00400000+0x00000000000249c6.	2019-07-04	not yet calculated	CVE-2019-13243 MISC
irfanview -- irfanview	IrfanView 4.52 has a User Mode Write AV starting at image00400000+0x00000000000013a98.	2019-07-04	not yet calculated	CVE-2019-13242 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jack_audio -- jack2	posix/JackSocket.cpp in libjack in JACK2 1.9.1 through 1.9.12 (as distributed with alsa-plugins 1.1.7 and later) has a "double file descriptor close" issue during a failed connection attempt when jackd2 is not running. Exploitation success depends on multithreaded timing of that double close, which can result in unintended information disclosure, crashes, or file corruption due to having the wrong file associated with the file descriptor.	2019-07-05	not yet calculated	CVE-2019-13351 MISC MISC
jetbrains -- hub	In JetBrains Hub versions earlier than 2018.4.11298, the audit events for SMTPSettings show a cleartext password to the admin user. It is only relevant in cases where a password has not changed since 2017, and if the audit log still contains events from before that period.	2019-07-03	not yet calculated	CVE-2019-12847 CONFIRM
jetbrains -- intellij_idea	In several JetBrains IntelliJ IDEA versions, creating remote run configurations of JavaEE application servers leads to saving a cleartext record of the server credentials in the IDE	2019-07-03	not yet calculated	CVE-2019-9823 CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configuration files. The issue has been fixed in the following versions: 2018.3.5, 2018.2.8, 2018.1.8.			FIRM
jetbrains -- intellij_idea	In several JetBrains IntelliJ IDEA versions, a Spring Boot run configuration with the default setting allowed remote attackers to execute code when the configuration is running, because a JMX server listens on all interfaces (instead of listening on only the localhost interface). This issue has been fixed in the following versions: 2019.1, 2018.3.4, 2018.2.8, 2018.1.8, and 2017.3.7.	2019-07-03	not yet calculated	CVE-2019-9186 CONFIRM
jetbrains -- intellij_idea	In several JetBrains IntelliJ IDEA Ultimate versions, an Application Server run configuration (for Tomcat, Jetty, Resin, or CloudBees) with the default setting allowed a remote attacker to execute code when the configuration is running, because a JMX server listened on all interfaces instead of localhost only. The issue has been fixed in the following versions: 2018.3.4, 2018.2.8, 2018.1.8, and 2017.3.7.	2019-07-03	not yet calculated	CVE-2019-10104 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- intellij_idea	JetBrains IntelliJ IDEA projects created using the Kotlin (JS Client/JVM Server) IDE Template were resolving Gradle artifacts using an http connection, potentially allowing an MITM attack. This issue, which was fixed in Kotlin plugin version 1.3.30, is similar to CVE-2019-10101.	2019-07-03	not yet calculated	CVE-2019-10103 CONFIRM
jetbrains -- intellij_idea_ultimate	In several versions of JetBrains IntelliJ IDEA Ultimate, creating run configurations for cloud application servers leads to saving a cleartext unencrypted record of the server credentials in the IDE configuration files. If the Settings Repository plugin was then used and configured to synchronize IDE settings using a public repository, these credentials were published to this repository. The issue has been fixed in the following versions: 2019.1, 2018.3.5, 2018.2.8, and 2018.1.8.	2019-07-03	not yet calculated	CVE-2019-9872 CONFIRM
jetbrains -- intellij_idea_ultimate	In several versions of JetBrains IntelliJ IDEA Ultimate, creating Task Servers configurations leads to saving a cleartext	2019-07-03	not yet calculated	CVE-2019-9873

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unencrypted record of the server credentials in the IDE configuration files. The issue has been fixed in the following versions: 2019.1, 2018.3.5, 2018.2.8, and 2018.1.8.			CONFIRM
jetbrains -- kotlin	JetBrains Ktor framework (created using the Kotlin IDE template) versions before 1.1.0 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack. This issue was fixed in Kotlin plugin version 1.3.30.	2019-07-03	not yet calculated	CVE-2019-10102 MISC
jetbrains -- kotlin	JetBrains Kotlin versions before 1.3.30 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack.	2019-07-03	not yet calculated	CVE-2019-10101 CONFIRM
jetbrains -- teamcity	A possible stored JavaScript injection requiring a deliberate server administrator action was detected. The issue was fixed in JetBrains TeamCity 2018.2.3.	2019-07-03	not yet calculated	CVE-2019-12843 CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				FIRM
jetbrains -- teamcity	Incorrect handling of user input in ZIP extraction was detected in JetBrains TeamCity. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	not yet calculated	CVE-2019-12841 CONFIRM
jetbrains -- teamcity	A possible stored JavaScript injection was detected on one of the JetBrains TeamCity pages. The issue was fixed in TeamCity 2018.2.3.	2019-07-03	not yet calculated	CVE-2019-12844 MISC
jetbrains -- youtrack	A query injection was possible in JetBrains YouTrack. The issue was fixed in YouTrack 2018.4.49168.	2019-07-03	not yet calculated	CVE-2019-12850 CONFIRM
jetbrains -- youtrack	Certain actions could cause privilege escalation for issue attachments in JetBrains	2019-	not yet calc	CVE-2019

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	YouTrack. The issue was fixed in 2018.4.49168.	07-03	ulated	- 12867 CONFIRM
jetbrains -- youtrack	In JetBrains YouTrack Confluence plugin versions before 1.8.1.3, it was possible to achieve Server Side Template Injection. The attacker could add an Issue macro to the page in Confluence, and use a combination of a valid id field and specially crafted code in the link-text-template field to execute code remotely.	2019-07-03	not yet calculated	CVE-2019-10100 MISC
jetbrains -- youtrack	A CSRF vulnerability was detected in one of the admin endpoints of JetBrains YouTrack. The issue was fixed in YouTrack 2018.4.49852.	2019-07-03	not yet calculated	CVE-2019-12851 CONFIRM
jetbrains -- youtrack	An SSRF attack was possible on a JetBrains YouTrack server. The issue (1 of 2) was fixed in JetBrains YouTrack 2018.4.49168.	2019-07-03	not yet calculated	CVE-2019-1285

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				2 CONFIRM
jetbrains -- youtrack	An Insecure Direct Object Reference, with Authorization Bypass through a User-Controlled Key, was possible in JetBrains YouTrack. The issue was fixed in 2018.4.49168.	2019-07-03	not yet calculated	CVE-2019-12866 CONFIRM
jgraph -- mxgraph	An issue was discovered in mxGraph through 4.0.0, related to the "draw.io Diagrams" plugin before 8.3.14 for Confluence and other products. Improper input validation/sanitization of a color field leads to XSS. This is associated with javascript/examples/grapheditor/www/js/Dialogs.js.	2019-07-01	not yet calculated	CVE-2019-13127 MISC MISC MISC
libosinfo -- libosinfo	libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to osinfo-install-script via the command line.	2019-07-05	not yet calculated	CVE-2019-13313 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC MISC
linux -- linux_kernel	In arch/x86/lib/insn-eval.c in the Linux kernel before 5.1.9, there is a use-after-free for access to an LDT entry because of a race condition between modify_ldt() and a #BR exception for an MPX bounds violation.	2019-07-04	not yet calculated	CVE-2019-13233 MISC MISC MISC MISC
linux -- linux_kernel	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a	2019-07-05	not yet calculated	CVE-2019-10638 MISC MISC MISC MISC MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.			CMISC MISC MISC
linux -- linux_kernel	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This attack can be carried out remotely, by the attacker forcing the target	2019-07-05	not yet calculated	CVE-2019-10639 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID generation was changed to have a dependency on an address associated with a network namespace.			
logitech -- r500_presentation_clicker	The Logitech R500 presentation clicker allows attackers to determine the AES key, leading to keystroke injection. On Windows, any text may be injected by using ALT+NUMPAD input to bypass the restriction on the characters A through Z.	2019-06-29	not yet calculated	CVE-2019-13054 MISC
logitech -- unifying_devices	Certain Logitech Unifying devices allow attackers to dump AES keys and addresses, leading to the	2019-06-29	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	capability of live decryption of Radio Frequency transmissions, as demonstrated by an attack against a Logitech K360 keyboard.		ulated	13055 MISC
logitech -- unifying_devices	Logitech Unifying devices before 2016-02-26 allow keystroke injection, bypassing encryption, aka MouseJack.	2019-06-29	not yet calculated	CVE-2016-10761 MISC MISC
logitech -- unifying_devices	Logitech Unifying devices allow live decryption if the pairing of a keyboard to a receiver is sniffed.	2019-06-29	not yet calculated	CVE-2019-13052 MISC
logitech -- unifying_devices	Logitech Unifying devices allow keystroke injection, bypassing encryption. The attacker must press a "magic" key combination while sniffing cryptographic data from a Radio Frequency transmission. NOTE: this issue exists because of an	2019-06-29	not yet calculated	CVE-2019-13053 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	incomplete fix for CVE-2016-10761.			
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Arbitrary file deletion.	2019-06-28	not yet calculated	CVE-2018-14916 MISC FULLDISC FULLDISC
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow XSS.	2019-06-28	not yet calculated	CVE-2018-14919 MISC FULLDISC FULLDISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Directory Traversal.	2019-06-28	not yet calculated	CVE-2018-14918 MISC FULLDISC
mcafee -- epolicy_orchestrator	Information Disclosure vulnerability in the Agent Handler in McAfee ePolicy Orchestrator (ePO) 5.9.x and 5.10.0 prior to 5.10.0 update 4 allows remote unauthenticated attacker to view sensitive information in plain text via sniffing the traffic between the Agent Handler and the SQL server.	2019-07-03	not yet calculated	CVE-2019-3619 CONFIRM
maxx -- waves_maxx_audio	WavesSysSvc in Waves MAXX Audio allows privilege escalation because the General registry key has Full Control access for the Users group, leading to DLL side loading. This affects WavesSysSvc64.exe 1.9.29.0.	2019-07-03	not yet calculated	CVE-2019-13208 MISC
medtronic -- minimed_508_and_paradigm	In Medtronic MinMed 508 and Medtronic Minimed	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_series_insulin_pumps	Paradigm Insulin Pumps, Versions, MiniMed 508 pump ? All versions, MiniMed Paradigm 511 pump ? All versions, MiniMed Paradigm 512/712 pumps ? All versions, MiniMed Paradigm 712E pump?All versions, MiniMed Paradigm 515/715 pumps?All versions, MiniMed Paradigm 522/722 pumps ? All versions,MiniMed Paradigm 522K/722K pumps ? All versions, MiniMed Paradigm 523/723 pumps ? Software versions 2.4A or lower, MiniMed Paradigm 523K/723K pumps ? Software, versions 2.4A or lower, MiniMed Paradigm Veo 554/754 pumps ? Software versions 2.6A or lower, MiniMed Paradigm Veo 554CM and 754CM models only ? Software versions 2.7A or lower, the affected insulin pumps are designed to communicate using a wireless RF with other devices, such as blood glucose meters, glucose sensor transmitters, and CareLink USB devices. This wireless RF communication protocol does not properly implement authentication or	06-28	calculated	2019-10964 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authorization. An attacker with adjacent access to one of the affected insulin pump models can inject, replay, modify, and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.			
mikrotik -- multiple_routers	A vulnerability in the FTP daemon on MikroTik routers through 6.44.3 could allow remote attackers to exhaust all available memory, causing the device to reboot because of uncontrolled resource management.	2019-07-03	not yet calculated	CVE-2019-13074 MISC
minicms -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the tags box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, and CVE-2018-20520.	2019-07-03	not yet calculated	CVE-2019-13186 MISC
ministry_of_interior_of_the_slovak_republic -- eid_client	An incorrect implementation of a local web server in eID client (Windows version before 3.1.2, Linux version before 3.0.3) allows remote attackers to execute arbitrary code (.cgi, .pl, or .php) or delete arbitrary files via a	2019-06-28	not yet calculated	CVE-2019-13028 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	crafted HTML page. This is a product from the Ministry of Interior of the Slovak Republic.			MISC MISC
motorola -- cx2l_mwr04l_router	On the Motorola router CX2L MWR04L 1.01, there is a stack consumption (infinite recursion) issue in scopd via TCP port 8010 and UDP port 8080. It is caused by snprintf and inappropriate length handling.	2019-07-01	not yet calculated	CVE-2019-13129 MISC
moxa -- oncell_g3100-hspa_series_devices	There is Memory corruption in the web interface Moxa OnCell G3100-HSPA Series version 1.6 Build 17100315 and prior, different vulnerability than CVE-2018-11420.	2019-07-03	not yet calculated	CVE-2018-11423 MISC
moxa -- oncell_g3100-hspa_series_devices	Moxa OnCell G3100-HSPA Series version 1.6 Build 17100315 and prior use a proprietary monitoring protocol that does not provide confidentiality, integrity, and authenticity security controls. All information is sent in plain text, and can be intercepted and modified. The protocol is vulnerable to remote unauthenticated disclosure of	2019-07-03	not yet calculated	CVE-2018-11421 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sensitive information, including the administrator's password. Under certain conditions, it's also possible to retrieve additional information, such as content of HTTP requests to the device, or the previously used password, due to memory leakages.			
moxa -- oncell_g3100-hspa_series_devices	A weak Cookie parameter is used in the web application of Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior. An attacker can brute force parameters required to bypass authentication and access the web interface to use all its functions except for password change.	2019-07-03	not yet calculated	CVE-2018-11426 MISC
moxa -- oncell_g3100-hspa_series_devices	CSRF tokens are not used in the web application of Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior, which makes it possible to perform CSRF attacks on the device administrator.	2019-07-03	not yet calculated	CVE-2018-11427 MISC
moxa -- oncell_g3100-hspa_series_devices	There is Memory corruption in the web interface of Moxa OnCell G3100-HSPA Series version 1.5 Build 17042015	2019-07-03	not yet calc	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and prio,r a different vulnerability than CVE-2018-11423.		ulated	11420 MISC
moxa -- oncell_g3100-hspa_series_devices	Moxa OnCell G3100-HSPA Series version 1.6 Build 17100315 and prior use a proprietary configuration protocol that does not provide confidentiality, integrity, and authenticity security controls. All information is sent in plain text, and can be intercepted and modified. Any commands (including device reboot, configuration download or upload, or firmware upgrade) are accepted and executed by the device without authentication.	2019-07-03	not yet calculated	CVE-2018-11422 MISC
moxa -- oncell_g3470a-lte_series_devices	There is Memory corruption in the web interface of Moxa OnCell G3470A-LTE Series version 1.6 Build 18021314 and prior, a different vulnerability than CVE-2018-11425.	2019-07-03	not yet calculated	CVE-2018-11424 MISC
moxa -- oncell_g3470a-lte_series_devices	Memory corruption issue was discovered in Moxa OnCell G3470A-LTE Series	2019-	not yet calc	CVE-2018

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	version 1.6 Build 18021314 and prior, a different vulnerability than CVE-2018-11424.	07-03	ulated	-11425 MISC
nlnet_labs -- nsd	nsd-checkzone in NLnet Labs NSD 4.2.0 has a Stack-based Buffer Overflow in the dname_concatenate() function in dname.c.	2019-07-03	not yet calculated	CVE-2019-13207 MISC
nortek_security_and_control -- linear_emerge_50p/5000p_devices	Linear eMerge 50P/5000P devices allow Cookie Path Traversal.	2019-07-02	not yet calculated	CVE-2019-7267 MISC MISC
nortek_security_and_control -- linear_emerge_50p/5000p_devices	Linear eMerge 50P/5000P devices allow Unauthenticated File Upload.	2019-07-02	not yet calculated	CVE-2019-7268 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
npm -- fstream	fstream before 1.0.12 is vulnerable to Arbitrary File Overwrite. Extracting tarballs containing a hardlink to a file that already exists in the system, and a file that matches the hardlink, will overwrite the system's file with the contents of the extracted file. The fstream.DirWriter() function is vulnerable.	2019-07-02	not yet calculated	CVE-2019-13173 MISC MISC
odoo -- community_and_enterprise	Incorrect access control in the TransientModel framework in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated attackers to access data in transient records that they do not own by making an RPC call before garbage collection occurs.	2019-07-03	not yet calculated	CVE-2018-14866 CONFIRM
odoo -- community_and_enterprise	Improper sanitization of dynamic user expressions in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated privileged users to escape from the dynamic expression sandbox and execute arbitrary code on the hosting system.	2019-07-03	not yet calculated	CVE-2018-14860 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
odoo -- community_and_enterprise	Incorrect access control in the password reset component in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated users to reset the password of other users by being the first party to use the secure token.	2019-07-03	not yet calculated	CVE-2018-14859 CONFIRM
odoo_community_association -- dbfilter_from_header_module	The Odoo Community Association (OCA) dbfilter_from_header module makes Odoo 8.x, 9.x, 10.x, and 11.x vulnerable to ReDoS (regular expression denial of service) under certain circumstances.	2019-07-05	not yet calculated	CVE-2018-14733 CONFIRM MISC MISC MISC MISC
opencats -- opencats	lib/DocumentToText.php in OpenCats before 0.9.4-3 has XXE that allows remote users to read files on the underlying operating system. The attacker must upload a file in the docx or odt format.	2019-07-05	not yet calculated	CVE-2019-13358 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
panduit -- intravue	An insecure login process was discovered in Panduit IntraVUE before 3.2.0.	2019-06-29	not yet calculated	CVE-2019-13044 MISC
qemu -- qemu	qemu-bridge-helper.c in QEMU 4.0.0 does not ensure that a network interface name (obtained from bridge.conf or a --br=bridge option) is limited to the IFNAMSIZ size, which can lead to an ACL bypass.	2019-07-03	not yet calculated	CVE-2019-13164 MLIST MISC
read_the_docs -- read_the_docs	Read the Docs before 3.5.1 has an Open Redirect if certain user-defined redirects are used. This affects private instances of Read the Docs (in addition to the public readthedocs.org web sites).	2019-07-02	not yet calculated	CVE-2019-13175 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
riello -- netman_204	An issue was discovered in Riello NetMan 204 14-2 and 15-2. The issue is with the login script and wrongpass Python script used for authentication. When calling wrongpass, the variables $VAL0 and $VAL1 should be enclosed in quotes to prevent the potential for Bash command injection. Further to this, VAL0 and VAL1 should be sanitised to ensure they do not contain malicious characters. Passing it the username of '-' will cause it to time out and log the user in because of poor error handling. This will log the attacker in as an administrator where the telnet / ssh services can be enabled, and the credentials for local users can be reset. Also, login.cgi accepts the username as a GET parameter, so login can be achieved by browsing to the /cgi-bin/login.cgi?username=-%20a URI.	2019-07-03	not yet calculated	CVE-2017-6900 MISC MISC
sdl2_image -- sdl2_image	An exploitable heap-based buffer overflow vulnerability exists when loading a PCX file in SDL2_image, version 2.0.4. A missing error	2019-07-03	not yet calculated	CVE-2019-5051

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	handler can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.			MISC
sdl2_image -- sdl2_image	An exploitable integer overflow vulnerability exists when loading a PCX file in SDL2_image 2.0.4. A specially crafted file can cause an integer overflow, resulting in too little memory being allocated, which can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	2019-07-03	not yet calculated	CVE-2019-5052 MISC
sick -- msc800_devices	SICK MSC800 all versions prior to Version 4.0, the affected firmware versions contain a hard-coded customer account password.	2019-07-01	not yet calculated	CVE-2019-10979 BID MISC
sigil-ebook -- flightcrew	FlightCrew v0.9.2 and older are vulnerable to a directory traversal, allowing attackers to write arbitrary files via a ../ (dot dot slash) in a ZIP	2019-07-04	not yet calculated	CVE-2019-1324

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	archive entry that is mishandled during extraction.			1 MISC
sitebridge -- joruri_cms	Cross-site scripting vulnerability in Joruri CMS 2017 Release2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5967 MISC MISC
sitebridge -- joruri_mail	Open redirect vulnerability in Joruri Mail 2.1.4 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5965 MISC MISC
sitebridge -- joruri_mail	Joruri Mail 2.1.4 and earlier does not properly manage sessions, which allows remote attackers to impersonate an arbitrary user and alter/disclose the information via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5966 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sks_keyserver_network -- sks-keyserver_code_and_gnupg	Interaction between the sks-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.16, makes it risky to have a GnuPG keyserver configuration line referring to a host on the SKS keyserver network. Retrieving data from this network may cause a persistent denial of service, because of a Certificate Spamming Attack.	2019-06-29	not yet calculated	CVE-2019-13050 MISC
sony -- vaio_update	Improper download file verification vulnerability in VAIO Update 7.3.0.03150 and earlier allows remote attackers to conduct a man-in-the-middle attack via a malicous wireless LAN access point. A successful exploitation may result in a malicious file being downloaded/executed.	2019-07-05	not yet calculated	CVE-2019-5982 MISC MISC
sony -- vaio_update	Improper authorization vulnerability in VAIO Update 7.3.0.03150 and earlier allows an attackers to execute arbitrary executable file with administrative privilege via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5981 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
squid-cache -- squid	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.	2019-07-05	not yet calculated	CVE-2019-13345 MISC MISC MLIST
stormshield -- stormshield_network_security	Stormshield Network Security 2.0.0 through 2.13.0 and 3.0.0 through 3.7.1 has self-XSS in the command line interface of the SNS web server.	2019-07-04	not yet calculated	CVE-2018-20850 MISC
supermicro -- superdoctor_5	Super Micro SuperDoctor 5, when restrictions are not implemented in agent.cfg, allows remote attackers to execute arbitrary commands via NRPE.	2019-07-01	not yet calculated	CVE-2019-13131 MISC
swift -- alliance_web_platform	An issue was discovered in SWIFT Alliance Web Platform 7.1.23. A log injection (and an arbitrary log filename) can be	2019-07-05	not yet calculated	CVE-2018-1638

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	achieved via the PATH_INFO to swp/login/EJBRemoteService/, related to com.swift.ejbgwt.j2ee.client.EjBlnvocationException error log information containing null@java:comp/env/ error messages.			6 MISC
tencent -- habo	HaboMalHunter through 2.0.0.3 in Tencent Habo allows attackers to evade dynamic malware analysis via PIE compilation.	2019-07-01	not yet calculated	CVE-2019-13125 MISC
tor_project -- tor_browser	Tor Browser through 8.5.3 has an information exposure vulnerability. It allows remote attackers to detect the browser's language via vectors involving an IFRAME element, because text in that language is included in the title attribute of a LINK element for a non-HTML page. This is related to a behavior of Firefox before 68.	2019-06-30	not yet calculated	CVE-2019-13075 MISC MISC
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the Private Port in Add Virtual Server.	07-02	calculated	2019-13153 MISC
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the IP Address in Add Gaming Rule.	2019-07-02	not yet calculated	CVE-2019-13152 MISC
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the UDP Ports To Open in Add Gaming Rule.	2019-07-02	not yet calculated	CVE-2019-13148 MISC
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the key	2019-07-02	not yet calculated	CVE-2019-13149 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	passwd in Routing RIP Settings.			
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the IP Address in Add Virtual Server.	2019-07-02	not yet calculated	CVE-2019-13155 MISC
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication). The command injection exists in the key ip_addr.	2019-07-02	not yet calculated	CVE-2019-13150 MISC
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the action set_sta_enrollee_pin_5g and the key wps_sta_enrollee_pin.	2019-07-02	not yet calculated	CVE-2019-13151 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the TCP Ports To Open in Add Gaming Rule.	2019-07-02	not yet calculated	CVE-2019-13154 MISC
tsukurito -- tootdon_for_mastodon	The Android App 'Tootdon for Mastodon' version 3.4.1 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-07-05	not yet calculated	CVE-2019-5961 MISC MISC
unzip -- unzip	Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a "better zip bomb" issue.	2019-07-04	not yet calculated	CVE-2019-13232 MISC MLIST MISC
virt-manager -- virt-boostrap	virt-bootstrap 1.1.0 allows local users to discover a root password by listing a	2019-	not yet calc	CVE-2019

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	process, because this password may be present in the --root-password option to virt_bootstrap.py.	07-05	ulated	- 13314 MISC MISC
virt-manager -- virt-manager	Virt-install(1) utility used to provision new virtual machines has introduced an option '--unattended' to create VMs without user interaction. This option accepts guest VM password as command line arguments, thus leaking them to others users on the system via process listing. It was introduced recently in the virt-manager v2.2.0 release.	2019-07-03	not yet calculated	CVE-2019-10183 BID CONFIRM
weberp -- weberp	A SQL Injection issue was discovered in webERP 4.15. Payments.php accepts payment data in base64 format. After this is decoded, it is deserialized. Then, this deserialized data goes directly into a SQL query, with no sanitizing checks.	2019-07-04	not yet calculated	CVE-2019-13292 MISC
weseek -- growi	Cross-site request forgery (CSRF) vulnerability in GROWI v3.4.6 and earlier allows remote attackers to	2019-07-05	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	hijack the authentication of administrators via updating user's 'Basic Info'.		ulated	5968 MISC MISC
weseek -- growi	Open redirect vulnerability in GROWI v3.4.6 and earlier allows remote attackersto redirect users to arbitrary web sites and conduct phishing attacks via the process of login.	2019-07-05	not yet calculated	CVE-2019-5969 MISC MISC
wolfvision -- cynap	WolfVision Cynap before 1.30j uses a static, hard-coded cryptographic secret for generating support PINs for the 'forgot password' feature. By knowing this static secret and the corresponding algorithm for calculating support PINs, an attacker can reset the ADMIN password and thus gain remote access.	2019-07-05	not yet calculated	CVE-2019-13352 MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to hijack the authentication of	2019-07-05	not yet calculated	CVE-2019-5971 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrators via unspecified vectors.			MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5962 MISC MISC
wordpress -- wordpress	A Cross-Site-Request-Forgery (CSRF) vulnerability in widget_logic.php in the 2by2host Widget Logic plugin before 5.10.2 for WordPress allows remote attackers to execute PHP code via snippets (that are attached to widgets and then eval'd to dynamically determine their visibility) by crafting a malicious POST request that tricks administrators into adding the code.	2019-07-01	not yet calculated	CVE-2019-12826 MISC CONFIRM
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Personalized WooCommerce Cart Page 2.4 and earlier	2019-07-05	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows remote attackers to hijack the authentication of administrators via unspecified vectors.		ulated	5979 MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5970 MISC MISC MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Contest Gallery versions prior to 10.4.5 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5974 MISC MISC
wordpress -- wordpress	An authentication bypass vulnerability in the CRUDLab WP Like Button plugin through 1.6.0 for WordPress allows unauthenticated attackers to change settings. The contains() function in	2019-07-05	not yet calculated	CVE-2019-13344 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	wp_like_button.php did not check if the current request is made by an authorized user, thus allowing any unauthenticated user to successfully update settings, as demonstrated by the wp-admin/admin.php?page=facebook-like-button each_page_url or code_snippet parameter.			MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in WP Open Graph 1.6.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5960 JVN
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5963 MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to inject arbitrary	2019-07-05	not yet calculated	CVE-2019-5972 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	web script or HTML via unspecified vectors.			CMISC MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Related YouTube Videos versions prior to 1.9.9 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5980 MISC MISC
wordpress -- wordpress	An issue was discovered in the VeronaLabs wp-statistics plugin before 12.6.7 for WordPress. The v1/hit endpoint of the API, when the non-default "use cache plugin" setting is enabled, is vulnerable to unauthenticated blind SQL Injection.	2019-07-04	not yet calculated	CVE-2019-13275 MISC MISC MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to hijack the authentication of	2019-07-05	not yet calculated	CVE-2019-5973 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrators via unspecified vectors.			MISC MISC
wuhan_deepin_technology -- deepin-clone	In GUI mode, deepin-clone before 1.1.3 creates a log file at the fixed path /tmp/.deepin-clone.log as root, and follows symlinks there. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled.	2019-07-04	not yet calculated	CVE-2019-13227 MLIST MISC MISC
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a fixed path /tmp/partclone.log in the Helper::getPartitionSizeInfo() function to write a log file as root, and follows symlinks there. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled.	2019-07-04	not yet calculated	CVE-2019-13229 MLIST MISC MISC
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a predictable path /tmp/.deepin-clone/mount/<block-dev-basename> in the	2019-07-04	not yet calculated	CVE-2019-1322

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Helper::temporaryMountDevice() function to temporarily mount a file system as root. An unprivileged user can prepare a symlink at this location to have the file system mounted in an arbitrary location. By winning a race condition, the attacker can also enter the mount point, thereby preventing a subsequent unmount of the file system.			6 MLIST MISC MISC
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a fixed path /tmp/repo.iso in the BootDoctor::fix() function to download an ISO file, and follows symlinks there. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled. By winning a race condition to replace the /tmp/repo.iso symlink by an attacker controlled ISO file, further privilege escalation may be possible.	2019-07-04	not yet calculated	CVE-2019-13228 MLIST MISC MISC
xpdf -- xpdf	In Xpdf 4.01.01, there is an out-of-bounds read vulnerability in the function SplashXPath::strokeAdjust()	2019-07-04	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	located at splash/SplashXPath.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an attacker to cause Information Disclosure. This is related to CVE-2018-16368.		ulated	13287 MISC
xpdf -- xpdf	In Xpdf 4.01.01, a heap-based buffer overflow could be triggered in DCTStream::decodeImage() in Stream.cc when writing to frameBuf memory. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service, an information leak, or possibly unspecified other impact.	2019-07-04	not yet calculated	CVE-2019-13281 MISC
xpdf -- xpdf	In Xpdf 4.01.01, there is a heap-based buffer over-read in the function JBIG2Stream::readTextRegionSeg() located at JBIG2Stream.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an	2019-07-04	not yet calculated	CVE-2019-13286 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to cause Information Disclosure.			
xpdf -- xpdf	In Xpdf 4.01.01, a heap-based buffer over-read could be triggered in SampledFunction::transform in Function.cc when using a large index for samples. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact.	2019-07-04	not yet calculated	CVE-2019-13282 MISC
xpdf -- xpdf	In Xpdf 4.01.01, there is a heap-based buffer over-read in the function DCTStream::readScan() located at Stream.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftops tool. It might allow an attacker to cause Information Disclosure.	2019-07-04	not yet calculated	CVE-2019-13291 MISC
xpdf -- xpdf	In Xpdf 4.01.01, the Parser::getObj() function in Parser.cc may cause infinite recursion via a crafted file. A remote attacker can leverage	2019-07-04	not yet calculated	CVE-2019-1328

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this for a DoS attack. This is similar to CVE-2018-16646.			8 MISC
xpdf -- xpdf	In Xpdf 4.01.01, there is a use-after-free vulnerability in the function JBIG2Stream::close() located at JBIG2Stream.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool.	2019-07-04	not yet calculated	CVE-2019-13289 MISC
xpdf -- xpdf	In Xpdf 4.01.01, a heap-based buffer over-read could be triggered in strncpy from FoFiType1::parse in fofi/FoFiType1.cc because it does not ensure the source string has a valid length before making a fixed-length copy. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact.	2019-07-04	not yet calculated	CVE-2019-13283 MISC