National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 Feb - 15 Feb 2019 Vol. 06 No. 03

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Advantech					
Webaccess/scada					
N/A	2019-02-05	7.5	WebAccess/SCADA, Version 8.3. An improper authentication vulnerability exists that could allow a possible authentication bypass allowing an attacker to upload malicious data. **CVE ID : CVE-2019-6519**	N/A	A-ADV-WEBA-020419/1
N/A	2019-02-05	7.5	WebAccess/SCADA, Version 8.3. Specially crafted requests could allow a possible authentication bypass that could allow an attacker to obtain and manipulate sensitive information. **CVE ID : CVE-2019-6521**	N/A	A-ADV-WEBA-020419/2
N/A	2019-02-05	7.5	WebAccess/SCADA, Version 8.3. The software does not properly sanitize its inputs for SQL commands. **CVE ID : CVE-2019-6523**	N/A	A-ADV-WEBA-020419/3
aioxmpp_project					
aioxmpp					
N/A	2019-02-04	5.8	aioxmpp version 0.10.2 and earlier contains a Improper Handling of Structural Elements vulnerability in Stanza Parser, rollback during	N/A	A-AIO-AIOX-020419/4

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			error processing, aioxmpp.xso.model.guard function that can result in Denial of Service, Other. This attack appears to be exploitable via Remote. A crafted stanza can be sent to an application which uses the vulnerable components to either inject data in a different context or cause the application to reconnect (potentially losing data). This vulnerability appears to have been fixed in 0.10.3. **CVE ID : CVE-2019-1000007**		
api-platform					
core					
N/A	2019-02-04	5.5	API Platform version from 2.2.0 to 2.3.5 contains an Incorrect Access Control vulnerability in GraphQL delete mutations that can result in a user authorized to delete a resource can delete any resource. This attack appears to be exploitable via the user must be authorized. This vulnerability appears to have been fixed in 2.3.6. **CVE ID : CVE-2019-1000011**	N/A	A-API-CORE-020419/5
articatech					
artica_proxy					
N/A	2019-02-01	9	Artica Proxy 3.06.200056 allows remote attackers to execute arbitrary commands	N/A	A-ART-ARTI-020419/6

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as root by reading the ressources/settings.inc ldap_admin and ldap_password fields, using these credentials at logon.php, and then entering the commands in the admin.index.php command-line field. **CVE ID : CVE-2019-7300**		
aveva					
indusoft_web_studio					
N/A	2019-02-12	10	AVEVA Software, LLC InduSoft Web Studio prior to Version 8.1 SP3 and InTouch Edge HMI (formerly InTouch Machine Edition) prior to Version 2017 Update. Code is executed under the program runtime privileges, which could lead to the compromise of the machine. **CVE ID : CVE-2019-6543**	N/A	A-AVE-INDU-020419/7
N/A	2019-02-12	10	AVEVA Software, LLC InduSoft Web Studio prior to Version 8.1 SP3 and InTouch Edge HMI (formerly InTouch Machine Edition) prior to Version 2017 Update. An unauthenticated remote user could use a specially crafted database connection configuration file to execute an arbitrary process on the server machine. **CVE ID : CVE-2019-6545**	N/A	A-AVE-INDU-020419/8
intouch_machine_edition_2014					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-12	10	AVEVA Software, LLC InduSoft Web Studio prior to Version 8.1 SP3 and InTouch Edge HMI (formerly InTouch Machine Edition) prior to Version 2017 Update. Code is executed under the program runtime privileges, which could lead to the compromise of the machine. **CVE ID : CVE-2019-6543**	N/A	A-AVE-INTO-020419/9
N/A	2019-02-12	10	AVEVA Software, LLC InduSoft Web Studio prior to Version 8.1 SP3 and InTouch Edge HMI (formerly InTouch Machine Edition) prior to Version 2017 Update. An unauthenticated remote user could use a specially crafted database connection configuration file to execute an arbitrary process on the server machine. **CVE ID : CVE-2019-6545**	N/A	A-AVE-INTO-020419/10
axiositalia					
registro_elettronico					
N/A	2019-02-10	4.3	Axios Italia Axios RE 1.7.0/7.0.0 devices have XSS via the RELogOff.aspx Error_Parameters parameter. In some situations, the XSS would be on the family.axioscloud.it cloud service; however, the vendor also supports "Sissi in Rete (con server)" for offline operation.	N/A	A-AXI-REGI-020419/11

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7693		
axiosys					
bento4					
N/A	2019-02-10	4.3	An issue was discovered in Bento4 v1.5.1-627. There is an assertion failure in AP4_AtomListWriter::Action in Core/Ap4Atom.cpp, leading to a denial of service (program crash), as demonstrated by mp42hls. **CVE ID : CVE-2019-7697**	N/A	A-AXI-BENT-020419/12
N/A	2019-02-10	4.3	An issue was discovered in AP4_Array<AP4_CttsTableEntry>::EnsureCapacity in Core/Ap4Array.h in Bento4 1.5.1-627. Crafted MP4 input triggers an attempt at excessive memory allocation, as demonstrated by mp42hls, a related issue to CVE-2018-20095. **CVE ID : CVE-2019-7698**	N/A	A-AXI-BENT-020419/13
N/A	2019-02-10	4.3	A heap-based buffer over-read occurs in AP4_BitStream::WriteBytes in Codecs/Ap4BitStream.cpp in Bento4 v1.5.1-627. Remote attackers could leverage this vulnerability to cause an exception via crafted mp4 input, which leads to a denial of service. **CVE ID : CVE-2019-7699**	N/A	A-AXI-BENT-020419/14
baijiacms_project					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
baijiacms					
N/A	2019-02-07	7.5	An issue was discovered in baijiacms V4 that can result in time-based blind SQL injection to get data via the cate parameter in an index.php?act=index request. **CVE ID : CVE-2019-7568**	N/A	A-BAI-BAIJ-020419/15
beescms					
beescms					
N/A	2019-02-15	6.8	BEESCMS 4.0 has a CSRF vulnerability to add arbitrary VIP accounts via the admin/admin_member.php?action=add&nav=add_web_user&admin_p_nav=user URI. **CVE ID : CVE-2019-8347**	N/A	A-BEE-BEES-020419/16
bijiadao					
waimai_super_cms					
N/A	2019-02-07	4.3	An issue was discovered in Waimai Super Cms 20150505. admin.php?m=Member&a=adminaddsave has XSS via the username or password parameter. **CVE ID : CVE-2019-7567**	N/A	A-BIJ-WAIM-020419/17
N/A	2019-02-07	7.5	An issue was discovered in Waimai Super Cms 20150505. web/Lib/Action/PublicAction.class.php allows time-based SQL Injection via the param array parameter to the /index.php?m=public&a=checkemail URI.	N/A	A-BIJ-WAIM-020419/18

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7585		
bo-blog					
bw					
N/A	2019-02-07	7.5	Bo-blog Wind through 1.6.0-r allows SQL Injection via the admin.php/comments/batchdel/ comID parameter because this parameter is mishandled in the mode/admin.mode.php delBlockedBatch function. **CVE ID : CVE-2019-7587**	N/A	A-BO--BW-020419/19
boolector_project					
boolector					
N/A	2019-02-07	4.3	In parser/btorsmt2.c in Boolector 3.0.0, opening a specially crafted input file leads to a use after free in get_failed_assumptions or btor_delete. **CVE ID : CVE-2019-7560**	N/A	A-BOO-BOOL-020419/20
btor2tools_project					
btor2tools					
N/A	2019-02-07	4.3	In btor2parser/btor2parser.c in Boolector Btor2Tools before 2019-01-15, opening a specially crafted input file leads to an out of bounds write in pusht_bfr. **CVE ID : CVE-2019-7559**	N/A	A-BTO-BTOR-020419/21
Buildbot					
Buildbot					
N/A	2019-02-03	5.8	www/resource.py in Buildbot before 1.8.1 allows CRLF injection in the Location	N/A	A-BUI-BUIL-020419/22

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			header of /auth/login and /auth/logout via the redirect parameter. This affects other web sites in the same domain. **CVE ID : CVE-2019-7313**		
Chamilo					
chamilo_lms					
N/A	2019-02-04	4.3	Chamilo Chamilo-lms version 1.11.8 and earlier contains a Cross Site Scripting (XSS) vulnerability in main/messages/new_message.php, main/social/personal_data.php, main/inc/lib/TicketManager.php, main/ticket/ticket_details.php that can result in a message being sent to the Administrator with the XSS to steal cookies. A ticket can be created with a XSS payload in the subject field. This attack appears to be exploitable via <svg/onload=alert(1)> as the payload user on the Subject field. This makes it possible to obtain the cookies of all users that have permission to view the tickets. This vulnerability appears to have been fixed in 1.11.x after commit 33e2692a37b5b6340cf5bec1a84e541460983c03. **CVE ID : CVE-2019-1000015**	N/A	A-CHA-CHAM-020419/23

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-04	4	Chamilo Chamilo-lms version 1.11.8 and earlier contains an Incorrect Access Control vulnerability in Tickets component that can result in an authenticated user can read all tickets available on the platform, due to lack of access controls. This attack appears to be exploitable via ticket_id=[ticket number]. This vulnerability appears to have been fixed in 1.11.x after commit 33e2692a37b5b6340cf5bec1a84e541460983c03. **CVE ID : CVE-2019-1000017**	N/A	A-CHA-CHAM-020419/24
cim_project					
cim					
N/A	2019-02-10	7.5	install/install.php in CIM 0.9.3 allows remote attackers to execute arbitrary PHP code via a crafted prefix value because of configuration file mishandling in the N=83 case, as demonstrated by a call to the PHP fputs function that creates a .php file in the public folder. **CVE ID : CVE-2019-7692**	N/A	A-CIM-CIM-020419/25
Cisco					
webex_meetings_online					
N/A	2019-02-07	4.3	A vulnerability in Cisco Webex Business Suite could allow an unauthenticated, remote attacker to inject arbitrary text	N/A	A-CIS-WEBE-020419/26

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			into a user's browser. The vulnerability is due to improper validation of input. An attacker could exploit this vulnerability by convincing a targeted user to view a malicious URL. A successful exploit could allow the attacker to inject arbitrary text into the user's browser. The attacker could use the content injection to conduct spoofing attacks. Versions prior than 3.0.9 are affected. **CVE ID : CVE-2019-1680**		
firepower_management_center					
N/A	2019-02-07	4.3	A vulnerability 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 system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute	N/A	A-CIS-FIRE-020419/27

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2019-1671**		
telepresence_management_suite					
N/A	2019-02-07	5	A vulnerability in the Simple Object Access Protocol (SOAP) of Cisco TelePresence Management Suite (TMS) software could allow an unauthenticated, remote attacker to gain unauthorized access to an affected device. The vulnerability is due to a lack of proper access and authentication controls on the affected TMS software. An attacker could exploit this vulnerability by gaining access to internal, trusted networks to send crafted SOAP calls to the affected device. If successful, an exploit could allow the attacker to access system management tools. Under normal circumstances, this access should be prohibited. **CVE ID : CVE-2019-1660**	N/A	A-CIS-TELE-020419/28
N/A	2019-02-07	4.3	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) software could allow an unauthenticated, remote attacker to conduct a cross-	N/A	A-CIS-TELE-020419/29

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. **CVE ID : CVE-2019-1661**		
web_security_appliance					
N/A	2019-02-08	5	A vulnerability in the Decryption Policy Default Action functionality of the Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to bypass a configured drop policy and allow traffic onto the network that should have been denied. The vulnerability is due to the incorrect handling of SSL-encrypted traffic when Decrypt for End-User Notification is disabled in the configuration. An attacker could exploit this vulnerability by sending a SSL connection	N/A	A-CIS-WEB_-020419/30

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through the affected device. A successful exploit could allow the attacker to bypass a configured drop policy to block specific SSL connections. Releases 10.1.x and 10.5.x are affected. **CVE ID : CVE-2019-1672**		
identity_services_engine					
N/A	2019-02-08	3.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient input validation of some parameters passed to the web-based management interface. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. For information about fixed software releases, consult the Cisco bug ID at https://quickview.cloudapps.cisco.com/quickview/bug/CSCvn64652. When considering	N/A	A-CIS-IDEN-020419/31

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution. **CVE ID : CVE-2019-1673**		
meeting_server					
N/A	2019-02-08	5	A vulnerability in the Session Initiation Protocol (SIP) call processing of Cisco Meeting Server (CMS) software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition of the Cisco Meeting Server. The vulnerability is due to insufficient validation of Session Description Protocol (SDP) messages. An attacker could exploit this vulnerability by sending a crafted SDP message to the CMS call bridge. An exploit could allow the attacker to cause the CMS to reload, causing a DoS condition for all connected clients. Versions prior to 2.3.9 are affected. **CVE ID : CVE-2019-1676**	N/A	A-CIS-MEET-020419/32
N/A	2019-02-07	4	A vulnerability in Cisco Meeting Server could allow an authenticated, remote attacker to cause a partial denial of service (DoS) to Cisco	N/A	A-CIS-MEET-020419/33

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Meetings application users who are paired with a Session Initiation Protocol (SIP) endpoint. The vulnerability is due to improper validation of coSpaces configuration parameters. An attacker could exploit this vulnerability by inserting crafted strings in specific coSpace parameters. An exploit could allow the attacker to prevent clients from joining a conference call in the affected coSpace. Versions prior to 2.4.3 are affected. **CVE ID : CVE-2019-1678**		
webex_meetings					
N/A	2019-02-07	1.9	A vulnerability in Cisco Webex Meetings for Android could allow an unauthenticated, local attacker to perform a cross-site scripting attack against the application. The vulnerability is due to insufficient validation of the application input parameters. An attacker could exploit this vulnerability by sending a malicious request to the Webex Meetings application through an intent. A successful exploit could allow the attacker to execute script code in the context of the Webex Meetings application. Versions prior to 11.7.0.236 are affected.	N/A	A-CIS-WEBE-020419/34

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1677		
telepresence_conductor					
N/A	2019-02-07	4	A vulnerability in the web interface of Cisco TelePresence Conductor, Cisco Expressway Series, and Cisco TelePresence Video Communication Server (VCS) Software could allow an authenticated, remote attacker to trigger an HTTP request from an affected server to an arbitrary host. This type of attack is commonly referred to as server-side request forgery (SSRF). The vulnerability is due to insufficient access controls for the REST API of Cisco Expressway Series and Cisco TelePresence VCS. An attacker could exploit this vulnerability by submitting a crafted HTTP request to the affected server. Versions prior to XC4.3.4 are affected. **CVE ID : CVE-2019-1679**	N/A	A-CIS-TELE-020419/35
telepresence_video_communication_server					
N/A	2019-02-07	4	A vulnerability in the web interface of Cisco TelePresence Conductor, Cisco Expressway Series, and Cisco TelePresence Video Communication Server (VCS) Software could allow an authenticated, remote attacker to trigger an HTTP request from an affected server to an arbitrary host. This type of attack is commonly referred to	N/A	A-CIS-TELE-020419/36

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as server-side request forgery (SSRF). The vulnerability is due to insufficient access controls for the REST API of Cisco Expressway Series and Cisco TelePresence VCS. An attacker could exploit this vulnerability by submitting a crafted HTTP request to the affected server. Versions prior to XC4.3.4 are affected. **CVE ID : CVE-2019-1679**		
network_assurance_engine					
N/A	2019-02-12	5.6	A vulnerability in the management web interface of Cisco Network Assurance Engine (NAE) could allow an unauthenticated, local attacker to gain unauthorized access or cause a Denial of Service (DoS) condition on the server. The vulnerability is due to a fault in the password management system of NAE. An attacker could exploit this vulnerability by authenticating with the default administrator password via the CLI of an affected server. A successful exploit could allow the attacker to view potentially sensitive information or bring the server down, causing a DoS condition. This vulnerability affects Cisco Network Assurance Engine (NAE) Release 3.0(1). The default password condition only	N/A	A-CIS-NETW-020419/37

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects new installations of Release 3.0(1). **CVE ID : CVE-2019-1688**		
css-tricks					
chat2					
N/A	2019-02-04	7.5	An issue was discovered in CSS-TRICKS Chat2 through 2015-05-05. The userid parameter in jumpin.php has a SQL injection vulnerability. **CVE ID : CVE-2019-7316**	N/A	A-CSS-CHAT-020419/38
cszcms					
csz_cms					
N/A	2019-02-07	6.8	CSZ CMS 1.1.8 has CSRF via admin/users/new/add. **CVE ID : CVE-2019-7566**	N/A	A-CSZ-CSZ_-020419/39
dbninja					
dbninja					
N/A	2019-02-06	3.5	In DbNinja 3.2.7, the Add Host function of the Manage Hosts pages has a Stored Cross-site Scripting (XSS) vulnerability in the User Name field. **CVE ID : CVE-2019-7545**	N/A	A-DBN-DBNI-020419/40
N/A	2019-02-11	6.8	DbNinja 3.2.7 allows session fixation via the data.php sessid parameter. **CVE ID : CVE-2019-7747**	N/A	A-DBN-DBNI-020419/41
N/A	2019-02-11	4.3	_includes\online.php in DbNinja 3.2.7 allows XSS via the data.php task parameter if _users/admin/tasks.php exists.	N/A	A-DBN-DBNI-020419/42

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7748		
d-circle					
power_egg					
N/A	2019-02-13	7.5	Input validation issue in POWER EGG(Ver 2.0.1, Ver 2.02 Patch 3 and earlier, Ver 2.1 Patch 4 and earlier, Ver 2.2 Patch 7 and earlier, Ver 2.3 Patch 9 and earlier, Ver 2.4 Patch 13 and earlier, Ver 2.5 Patch 12 and earlier, Ver 2.6 Patch 8 and earlier, Ver 2.7 Patch 6 and earlier, Ver 2.7 Government Edition Patch 7 and earlier, Ver 2.8 Patch 6 and earlier, Ver 2.8c Patch 5 and earlier, Ver 2.9 Patch 4 and earlier) allows remote attackers to execute EL expression on the server via unspecified vectors. **CVE ID : CVE-2019-5916**	N/A	A-D-C-POWE-020419/43
Debian					
tmpreaper					
N/A	2019-02-04	4.4	Debian tmpreaper version 1.6.13+nmu1 has a race condition when doing a (bind) mount via rename() which could result in local privilege escalation. Mounting via rename() could potentially lead to a file being placed elsewhereon the filesystem hierarchy (e.g. /etc/cron.d/) if the directory being cleaned up was on the same physical	N/A	A-DEB-TMPR-020419/44

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			filesystem. Fixed versions include 1.6.13+nmu1+deb9u1 and 1.6.14. **CVE ID : CVE-2019-3461**		
Djangoproject					
Django					
N/A	2019-02-11	5	Django 1.11.x before 1.11.19, 2.0.x before 2.0.11, and 2.1.x before 2.1.6 allows Uncontrolled Memory Consumption via a malicious attacker-supplied value to the django.utils.numberformat.format() function. **CVE ID : CVE-2019-6975**	N/A	A-DJA-DJAN-020419/45
Docker					
Docker					
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.	N/A	A-DOC-DOCK-020419/46

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5736		
elfutils_project					
elfutils					
N/A	2019-02-09	4.3	In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an incorrect overflow check. Crafted elf input causes a segmentation fault, leading to denial of service (program crash). **CVE ID : CVE-2019-7664**	N/A	A-ELF-ELFU-020419/47
N/A	2019-02-09	4.3	In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatetom.c in libelf. A crafted ELF input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note does not reject malformed core file notes. **CVE ID : CVE-2019-7665**	N/A	A-ELF-ELFU-020419/48
Emsisoft					
Anti-malware					
N/A	2019-02-08	5	EPP.sys in Emsisoft Anti-Malware 2018.8.1.8923 allows an attacker to bypass ACLs because Interpreted Device Characteristics lacks FILE_DEVICE_SECURE_OPEN and therefore files and directories "inside" the \\.\EPP device are not	N/A	A-EMS-ANTI-020419/49

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly protected, leading to unintended impersonation or object creation. **CVE ID : CVE-2019-7651**		
Erlang					
rebar3					
N/A	2019-02-04	6.8	Erlang/OTP Rebar3 version 3.7.0 through 3.7.5 contains a Signing oracle vulnerability in Package registry verification that can result in Package modifications not detected, allowing code execution. This attack appears to be exploitable via Victim fetches packages from malicious/compromised mirror. This vulnerability appears to have been fixed in 3.8.0. **CVE ID : CVE-2019-1000014**	N/A	A-ERL-REBA-020419/50
Estrongs					
es_file_explorer_file_manager					
N/A	2019-02-15	4.3	The Help feature in the ES File Explorer File Manager application 4.1.9.7.4 for Android allows session hijacking by a Man-in-the-middle attacker on the local network because HTTPS is not used, and an attacker's web site is displayed in a WebView with no information about the URL. **CVE ID : CVE-2019-8345**	N/A	A-EST-ES_F-020419/51

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
F5					
big-ip_access_policy_manager					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/52
N/A	2019-02-05	3.5	On BIG-IP APM 14.0.0 to 14.0.0.4, 13.0.0 to 13.1.1.3 and 12.1.0 to 12.1.3.7, a reflected cross-site scripting (XSS) vulnerability exists in the resource information page for authenticated users when a full webtop is configured on the BIG-IP APM system. **CVE ID : CVE-2019-6591**	https://support.f5.com/csp/article/K32840424	A-F5-BIG--020419/53
big-ip_advanced_firewall_manager					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/54

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
big-ip_analytics					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/55
big-ip_application_acceleration_manager					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/56
big-ip_application_security_manager					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/57

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
big-ip_domain_name_system					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/58
big-ip_edge_gateway					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/59
big-ip_fraud_protection_service					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/60

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
big-ip_global_traffic_manager					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/61
big-ip_link_controller					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/62
big-ip_local_traffic_manager					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/63

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-05	7.1	On BIG-IP LTM 13.0.0 to 13.0.1 and 12.1.0 to 12.1.3.6, under certain conditions, the TMM may consume excessive resources when processing SSL Session ID Persistence traffic. **CVE ID : CVE-2019-6590**	https://support.f5.com/csp/article/K55101404	A-F5-BIG--020419/64
big-ip_policy_enforcement_manager					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/65
big-ip_webaccelerator					
N/A	2019-02-13	4.3	On BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, and 11.6.0-11.6.3.2, a reflected Cross Site Scripting (XSS) vulnerability is present in an undisclosed page of the BIG-IP TMUI (Traffic Management User Interface) also known as the BIG-IP configuration utility. **CVE ID : CVE-2019-6589**	https://support.f5.com/csp/article/K23566124	A-F5-BIG--020419/66
Ffmpeg					
Ffmpeg					
N/A	2019-02-04	4.3	FFMPEG version 4.1 contains a	N/A	A-FFM-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CWE-129: Improper Validation of Array Index vulnerability in libavcodec/cbs_av1.c that can result in Denial of service. This attack appears to be exploitable via specially crafted AV1 file has to be provided as input. This vulnerability appears to have been fixed in after commit b97a4b658814b2de8b9f2a3bce491c002d34de31. **CVE ID : CVE-2019-1000016**		FFMP-020419/67
Flatpak					
Flatpak					
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**	N/A	A-FLA-FLAT-020419/68
forcepoint					
user_id					
N/A	2019-02-07	7.5	Forcepoint User ID (FUID) server versions up to 1.2 have a remote arbitrary file upload vulnerability on TCP port 5001. Successful exploitation of this vulnerability may lead to remote code execution. To fix this vulnerability, upgrade to FUID version 1.3 or higher. To prevent the vulnerability on FUID versions 1.2 and below, apply local firewall	N/A	A-FOR-USER-020419/69

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rules on the FUID server to disable all external access to port TCP/5001. FUID requires this port only for local connections through the loopback interface. **CVE ID : CVE-2019-6139**		
Freebsd					
freebsd					
N/A	2019-02-12	2.1	In FreeBSD before 11.2-STABLE(r343782), 11.2-RELEASE-p9, 12.0-STABLE(r343781), and 12.0-RELEASE-p3, kernel callee-save registers are not properly sanitized before return from system calls, potentially allowing some kernel data used in the system call to be exposed. **CVE ID : CVE-2019-5595**	N/A	A-FRE-FREE-020419/70
N/A	2019-02-12	7.2	In FreeBSD 11.2-STABLE after r338618 and before r343786, 12.0-STABLE before r343781, and 12.0-RELEASE before 12.0-RELEASE-p3, a bug in the reference count implementation for UNIX domain sockets can cause a file structure to be incorrectly released potentially allowing a malicious local user to gain root privileges or escape from a jail. **CVE ID : CVE-2019-5596**	N/A	A-FRE-FREE-020419/71
Freedesktop					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Poppler					
N/A	2019-02-02	6.8	In Poppler 0.73.0, a heap-based buffer over-read (due to an integer signedness error in the XRef::getEntry function in XRef.cc) allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document, as demonstrated by pdftocairo. **CVE ID : CVE-2019-7310**	N/A	A-FRE-POPP-020419/72
genivia					
gsoap					
N/A	2019-02-09	6.8	Genivia gSOAP 2.7.x and 2.8.x before 2.8.75 allows attackers to cause a denial of service (application abort) or possibly have unspecified other impact if a server application is built with the -DWITH_COOKIES flag. This affects the C/C++ libgsoapck/libgsoapck++ and libgsoapssl/libgsoapssl++ libraries, as these are built with that flag. **CVE ID : CVE-2019-7659**	https://www.genivia.com/advisory.html#Bug_in_gSOAP_versions_2.7.0_to_2.8.74_for_applications_built_with_the_WITH_COOKIES_flag_enabled_(Jan_14,_2019)	A-GEN-GSOA-020419/73
gitea					
gitea					
N/A	2019-02-04	5.5	Gitea version 1.6.2 and earlier contains a Incorrect Access Control vulnerability in Delete/Edit file functionallity	N/A	A-GIT-GITE-020419/74

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that can result in the attacker deleting files outside the repository he/she has access to. This attack appears to be exploitable via the attacker must get write access to "any" repository including self-created ones.. This vulnerability appears to have been fixed in 1.6.3, 1.7.0-rc2. **CVE ID : CVE-2019-1000002**		
Gnome					
gnome_display_manager					
N/A	2019-02-06	6.9	A vulnerability was discovered in gdm before 3.31.4. When timed login is enabled in configuration, an attacker could bypass the lock screen by selecting the timed login user and waiting for the timer to expire, at which time they would gain access to the logged-in user's session. **CVE ID : CVE-2019-3825**	N/A	A-GNO-GNOM-020419/75
GNU					
Glibc					
N/A	2019-02-02	2.1	In the GNU C Library (aka glibc or libc6) through 2.29, the memcmp function for the x32 architecture can incorrectly return zero (indicating that the inputs are equal) because the RDX most significant bit is mishandled. **CVE ID : CVE-2019-7309**	N/A	A-GNU-GLIB-020419/76

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Google					
kubernetes_engine					
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe. **CVE ID : CVE-2019-5736**	N/A	A-GOO-KUBE-020419/77
Graphicsmagick					
Graphicsmagick					
N/A	2019-02-04	5	In ImageMagick before 7.0.8-25 and GraphicsMagick through 1.3.31, several memory leaks exist in WritePDFImage in coders/pdf.c. **CVE ID : CVE-2019-7397**	N/A	A-GRA-GRAP-020419/78
gsi-openssh_project					
gsi-openssh					
N/A	2019-02-08	4.3	An issue was discovered in gsi-openssh-server 7.9p1 on	N/A	A-GSI-GSI--020419/79

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Fedora 29. If PermitPAMUserChange is set to yes in the /etc/gsissh/sshd_config file, logins succeed with a valid username and an incorrect password, even though a failure entry is recorded in the /var/log/messages file. **CVE ID : CVE-2019-7639**		
Gurock					
Testrail					
N/A	2019-02-07	5	index.php in Gurock TestRail 5.3.0.3603 returns potentially sensitive information for an invalid request, as demonstrated by full path disclosure and the identification of PHP as the backend technology. **CVE ID : CVE-2019-7535**	N/A	A-GUR-TEST-020419/80
Haxx					
Libcurl					
N/A	2019-02-06	7.5	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented	N/A	A-HAX-LIBC-020419/81

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header. **CVE ID : CVE-2019-3822**		
N/A	2019-02-06	5	libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to \`smtp_endofresp()\` isn't NUL terminated and contains no character ending the parsed number, and \`len\` is set to 5, then the \`strtol()\` call reads beyond the allocated buffer. The read contents will not be returned to the caller. **CVE ID : CVE-2019-3823**	N/A	A-HAX-LIBC-020419/82
helm					
chartmuseum					
N/A	2019-02-04	4	Helm ChartMuseum version >=0.1.0 and < 0.8.1 contains a CWE-22: Improper Limitation	N/A	A-HEL-CHAR-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in HTTP API to save charts that can result in a specially crafted chart could be uploaded and saved outside the intended location. This attack appears to be exploitable via A POST request to the HTTP API can save a chart archive outside of the intended directory. If authentication is, optionally, enabled this requires an authorized user to do so. This vulnerability appears to have been fixed in 0.8.1. **CVE ID : CVE-2019-1000009**		020419/83
hex					
hex_core					
N/A	2019-02-04	6.8	Hex package manager hex_core version 0.3.0 and earlier contains a Signing oracle vulnerability in Package registry verification that can result in Package modifications not detected, allowing code execution. This attack appears to be exploitable via victim fetches packages from malicious/compromised mirror. This vulnerability appears to have been fixed in 0.4.0. **CVE ID : CVE-2019-1000013**	N/A	A-HEX-HEX_-020419/84

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hotels_server_project					
hotels_server					
N/A	2019-02-08	5	controller/fetchpwd.php and controller/doAction.php in Hotels_Server through 2018-11-05 rely on base64 in an attempt to protect password storage. **CVE ID : CVE-2019-7648**	N/A	A-HOT-HOTE-020419/85
housegate					
house_gate					
N/A	2019-02-13	5	Directory traversal vulnerability in HOUSE GATE App for iOS 1.7.8 and earlier allows remote attackers to read arbitrary files via unspecified vectors. **CVE ID : CVE-2019-5910**	N/A	A-HOU-HOUS-020419/86
HP					
onesphere					
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be	N/A	A-HP-ONES-020419/87

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe. **CVE ID : CVE-2019-5736**		
IBM					
api_connect					
N/A	2019-02-07	5	API Connect V2018.1 through 2018.4.1.1 is impacted by access token leak. Authorization tokens in some URLs can result in the tokens being written to log files. IBM X-Force ID: 155626. **CVE ID : CVE-2019-4008**	https://www.ibm.com/support/docview.wss?uid=ibm10869772	A-IBM-API_-020419/88
security_identity_manager					
N/A	2019-02-04	4.6	IBM Security Identity Manager 6.0 and 7.0 could allow an attacker to create unexpected control flow paths through the application, potentially bypassing security checks. Exploitation of this weakness can result in a limited form of code injection. IBM X-Force ID: 156162. **CVE ID : CVE-2019-4038**	https://www.ibm.com/support/docview.wss?uid=ibm10869604	A-IBM-SECU-020419/89
rational_clearcase					
N/A	2019-02-15	5	IBM Rational ClearCase 1.0.0.0 GIT connector does not sufficiently protect the document database password. An attacker could obtain the password and gain unauthorized access to the	https://www.ibm.com/support/docview.wss?uid=ibm10870810	A-IBM-RATI-020419/90

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			document database. IBM X-Force ID: 156583. **CVE ID : CVE-2019-4059**		
Imagemagick					
Imagemagick					
N/A	2019-02-04	5	In ImageMagick before 7.0.8-25, a memory leak exists in WritePSDChannel in coders/psd.c. **CVE ID : CVE-2019-7395**	N/A	A-IMA-IMAG-020419/91
N/A	2019-02-04	5	In ImageMagick before 7.0.8-25, a memory leak exists in ReadSIXELImage in coders/sixel.c. **CVE ID : CVE-2019-7396**	N/A	A-IMA-IMAG-020419/92
N/A	2019-02-04	5	In ImageMagick before 7.0.8-25 and GraphicsMagick through 1.3.31, several memory leaks exist in WritePDFImage in coders/pdf.c. **CVE ID : CVE-2019-7397**	N/A	A-IMA-IMAG-020419/93
N/A	2019-02-04	5	In ImageMagick before 7.0.8-25, a memory leak exists in WriteDIBImage in coders/dib.c. **CVE ID : CVE-2019-7398**	N/A	A-IMA-IMAG-020419/94
inxedu					
inxedu					
N/A	2019-02-09	10	inxedu through 2018-12-24 has a vulnerability that can lead to the upload of a malicious JSP file. The vulnerable code location is	N/A	A-INX-INXE-020419/95

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟥	com.inxedu.os.common.controller.VideoUploadController#gok4 (com/inxedu/os/common/controller/VideoUploadController.java). The attacker uses the /video/uploadvideo fileType parameter to change the list of acceptable extensions from jpg,gif,png,jpeg to jpg,gif,png,jsp,jpeg. **CVE ID : CVE-2019-7684**		
Jenkins					
script_security					
N/A	2019-02-06	6.5	A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.50 and earlier in src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/SecureGroovyScript.java that allows attackers with Overall/Read permission to provide a Groovy script to an HTTP endpoint that can result in arbitrary code execution on the Jenkins master JVM. **CVE ID : CVE-2019-1003005**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1292	A-JEN-SCRI-020419/96
groovy					
N/A	2019-02-06	6.5	A sandbox bypass vulnerability exists in Jenkins Groovy Plugin 2.0 and earlier in src/main/java/hudson/plugins/groovy/StringScriptSource.java that allows attackers with	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1293	A-JEN-GROO-020419/97

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Overall/Read permission to provide a Groovy script to an HTTP endpoint that can result in arbitrary code execution on the Jenkins master JVM. **CVE ID : CVE-2019-1003006**		
warnings					
N/A	2019-02-06	6.8	A cross-site request forgery vulnerability exists in Jenkins Warnings Plugin 5.0.0 and earlier in src/main/java/hudson/plugins/warnings/GroovyParser.java that allows attackers to execute arbitrary code via a form validation HTTP endpoint. **CVE ID : CVE-2019-1003007**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1295%20(1)	A-JEN-WARN-020419/98
warnings_next_generation					
N/A	2019-02-06	6.8	A cross-site request forgery vulnerability exists in Jenkins Warnings Next Generation Plugin 2.1.1 and earlier in src/main/java/io/jenkins/plugins/analysis/warnings/groovy/GroovyParser.java that allows attackers to execute arbitrary code via a form validation HTTP endpoint. **CVE ID : CVE-2019-1003008**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1295%20(2)	A-JEN-WARN-020419/99
N/A	2019-02-06	4.3	A cross-site scripting vulnerability exists in Jenkins Warnings Next Generation Plugin 1.0.1 and earlier in src/main/java/io/jenkins/plugins/analysis/core/model/Det	https://jenkins.io/security/advisory/2019-01-28/#SECU	A-JEN-WARN-020419/100

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ailsTableModel.java, src/main/java/io/jenkins/plugins/analysis/core/model/SourceDetail.java, src/main/java/io/jenkins/plugins/analysis/core/model/SourcePrinter.java, src/main/java/io/jenkins/plugins/analysis/core/util/Sanitizer.java, src/main/java/io/jenkins/plugins/analysis/warnings/DuplicateCodeScanner.java that allows attackers with the ability to control warnings parser input to have Jenkins render arbitrary HTML. **CVE ID : CVE-2019-1003023**	RITY-1271	
active_directory					
N/A	2019-02-06	5.8	An improper certificate validation vulnerability exists in Jenkins Active Directory Plugin 2.10 and earlier in src/main/java/hudson/plugins/active_directory/ActiveDirectoryDomain.java, src/main/java/hudson/plugins/active_directory/ActiveDirectorySecurityRealm.java, src/main/java/hudson/plugins/active_directory/ActiveDirectoryUnixAuthenticationProvider.java that allows attackers to impersonate the Active Directory server Jenkins connects to for authentication if Jenkins is configured to use	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-859	A-JEN-ACTI-020419/101

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			StartTLS. **CVE ID : CVE-2019-1003009**		
git					
N/A	2019-02-06	4.3	A cross-site request forgery vulnerability exists in Jenkins Git Plugin 3.9.1 and earlier in src/main/java/hudson/plugins/git/GitTagAction.java that allows attackers to create a Git tag in a workspace and attach corresponding metadata to a build record. **CVE ID : CVE-2019-1003010**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1095	A-JEN-GIT-020419/102
token_macro					
N/A	2019-02-06	5.5	An information exposure and denial of service vulnerability exists in Jenkins Token Macro Plugin 2.5 and earlier in src/main/java/org/jenkinsci/plugins/tokenmacro/Parser.java, src/main/java/org/jenkinsci/plugins/tokenmacro/TokenMacro.java, src/main/java/org/jenkinsci/plugins/tokenmacro/impl/AbstractChangesSinceMacro.java, src/main/java/org/jenkinsci/plugins/tokenmacro/impl/ChangesSinceLastBuildMacro.java, src/main/java/org/jenkinsci/plugins/tokenmacro/impl/ProjectUrlMacro.java that allows attackers with the ability to control token macro input (such as SCM changelogs) to	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1102	A-JEN-TOKE-020419/103

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			define recursive input that results in unexpected macro evaluation. **CVE ID : CVE-2019-1003011**		
blue_ocean					
N/A	2019-02-06	4.3	A data modification vulnerability exists in Jenkins Blue Ocean Plugins 1.10.1 and earlier in blueocean-core-js/src/js/bundleStartup.js, blueocean-core-js/src/js/fetch.ts, blueocean-core-js/src/js/i18n/i18n.js, blueocean-core-js/src/js/urlconfig.js, blueocean-rest/src/main/java/io/jenkins/blueocean/rest/APICrumbExclusion.java, blueocean-web/src/main/java/io/jenkins/blueocean/BlueOceanUI.java, blueocean-web/src/main/resources/io/jenkins/blueocean/BlueOceanUI/index.jelly that allows attackers to bypass all cross-site request forgery protection in Blue Ocean API. **CVE ID : CVE-2019-1003012**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1201	A-JEN-BLUE-020419/104
N/A	2019-02-06	3.5	An cross-site scripting vulnerability exists in Jenkins Blue Ocean Plugins 1.10.1 and earlier in blueocean-commons/src/main/java/io/jenkins/blueocean/commons/stapler/Export.java, blueocean-commons/src/main/java/io/j	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1204	A-JEN-BLUE-020419/105

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enkins/blueocean/commons/stapler/export/ExportConfig.java, blueocean-commons/src/main/java/io/jenkins/blueocean/commons/stapler/export/JSONDataWriter.java, blueocean-rest-impl/src/main/java/io/jenkins/blueocean/service/embedded/UserStatePreloader.java, blueocean-web/src/main/resources/io/jenkins/blueocean/PageStatePreloadDecorator/header.jelly that allows attackers with permission to edit a user's description in Jenkins to have Blue Ocean render arbitrary HTML when using it as that user. **CVE ID : CVE-2019-1003013**		
config_file_provider					
N/A	2019-02-06	3.5	An cross-site scripting vulnerability exists in Jenkins Config File Provider Plugin 3.4.1 and earlier in src/main/resources/lib/configfiles/configfiles.jelly that allows attackers with permission to define shared configuration files to execute arbitrary JavaScript when a user attempts to delete the shared configuration file. **CVE ID : CVE-2019-1003014**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1253	A-JEN-CONF-020419/106
job_import					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-06	6.4	An XML external entity processing vulnerability exists in Jenkins Job Import Plugin 2.1 and earlier in src/main/java/org/jenkins/ci/plugins/jobimport/client/RestApiClient.java that allows attackers with the ability to control the HTTP server (Jenkins) queried in preparation of job import to read arbitrary files, perform a denial of service attack, etc. **CVE ID : CVE-2019-1003015**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-905%20(1)	A-JEN-JOB_-020419/107
N/A	2019-02-06	4.3	An exposure of sensitive information vulnerability exists in Jenkins Job Import Plugin 2.1 and earlier in src/main/java/org/jenkins/ci/plugins/jobimport/JobImportAction.java, src/main/java/org/jenkins/ci/plugins/jobimport/JobImportGlobalConfig.java, src/main/java/org/jenkins/ci/plugins/jobimport/model/JenkinsSite.java that allows attackers with Overall/Read permission to have Jenkins connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-1003016**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-905%20(2)	A-JEN-JOB_-020419/108
N/A	2019-02-06	2.6	A data modification	https://jen	A-JEN-JOB_-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists in Jenkins Job Import Plugin 3.0 and earlier in JobImportAction.java that allows attackers to copy jobs from a preconfigured other Jenkins instance, potentially installing additional plugins necessary to load the imported job's configuration. **CVE ID : CVE-2019-1003017**	kins.io/security/advisory/2019-01-28/#SECURITY-1302	020419/109
github_oauth					
N/A	2019-02-06	4.3	An exposure of sensitive information vulnerability exists in Jenkins GitHub Authentication Plugin 0.29 and earlier in GithubSecurityRealm/config.jelly that allows attackers able to view a Jenkins administrator's web browser output, or control the browser (e.g. malicious extension) to retrieve the configured client secret. **CVE ID : CVE-2019-1003018**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-602	A-JEN-GITH-020419/110
N/A	2019-02-06	4.3	An session fixation vulnerability exists in Jenkins GitHub Authentication Plugin 0.29 and earlier in GithubSecurityRealm.java that allows unauthorized attackers to impersonate another user if they can control the pre-authentication session. **CVE ID : CVE-2019-1003019**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-797	A-JEN-GITH-020419/111

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
kanboard					
N/A	2019-02-06	4	A server-side request forgery vulnerability exists in Jenkins Kanboard Plugin 1.5.10 and earlier in KanboardGlobalConfiguration.java that allows attackers with Overall/Read permission to submit a GET request to an attacker-specified URL. **CVE ID : CVE-2019-1003020**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-818	A-JEN-KANB-020419/112
openid_connect_authentication					
N/A	2019-02-06	4.3	An exposure of sensitive information vulnerability exists in Jenkins OpenId Connect Authentication Plugin 1.4 and earlier in OicSecurityRealm/config.jelly that allows attackers able to view a Jenkins administrator's web browser output, or control the browser (e.g. malicious extension) to retrieve the configured client secret. **CVE ID : CVE-2019-1003021**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-886	A-JEN-OPEN-020419/113
monitoring					
N/A	2019-02-06	4.3	A denial of service vulnerability exists in Jenkins Monitoring Plugin 1.74.0 and earlier in PluginImpl.java that allows attackers to kill threads running on the Jenkins master. **CVE ID : CVE-2019-1003022**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1153	A-JEN-MONI-020419/114
Jforum					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Jforum					
N/A	2019-02-12	5	In JForum 2.1.8, an unauthenticated, remote attacker can enumerate whether a user exists by using the "create user" function. If a register/check/username?username= request corresponds to a username that exists, then an "is already in use" error is produced. NOTE: this product is discontinued. **CVE ID : CVE-2019-7550**	N/A	A-JFO-JFOR-020419/115
Joomla					
joomla					
N/A	2019-02-12	4.3	An issue was discovered in Joomla! before 3.9.3. The "No Filtering" textfilter overrides child settings in the Global Configuration. This is intended behavior. However, it might be unexpected for the user because the configuration dialog lacks an additional message to explain this. **CVE ID : CVE-2019-7739**	N/A	A-JOO-JOOM-020419/116
N/A	2019-02-12	4.3	An issue was discovered in Joomla! before 3.9.3. Inadequate parameter handling in JavaScript code (core.js writeDynaList) could lead to an XSS attack vector. **CVE ID : CVE-2019-7740**	N/A	A-JOO-JOOM-020419/117
N/A	2019-02-12	4.3	An issue was discovered in Joomla! before 3.9.3. Inadequate checks at the	N/A	A-JOO-JOOM-020419/118

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Global Configuration helpurl settings allowed stored XSS. **CVE ID : CVE-2019-7741**		
N/A	2019-02-12	4.3	An issue was discovered in Joomla! before 3.9.3. A combination of specific web server configurations, in connection with specific file types and browser-side MIME-type sniffing, causes an XSS attack vector. **CVE ID : CVE-2019-7742**	N/A	A-JOO-JOOM-020419/119
N/A	2019-02-12	7.5	An issue was discovered in Joomla! before 3.9.3. The phar:// stream wrapper can be used for objection injection attacks because there is no protection mechanism (such as the TYPO3 PHAR stream wrapper) to prevent use of the phar:// handler for non .phar-files. **CVE ID : CVE-2019-7743**	N/A	A-JOO-JOOM-020419/120
N/A	2019-02-12	4.3	An issue was discovered in Joomla! before 3.9.3. Inadequate filtering on URL fields in various core components could lead to an XSS vulnerability. **CVE ID : CVE-2019-7744**	N/A	A-JOO-JOOM-020419/121
jspmyadmin					
jspmyadmin2					
N/A	2019-02-04	4.3	yugandhargangu JspMyAdmin2 version 1.0.6 and earlier contains a Cross	N/A	A-JSP-JSPM-020419/122

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Site Scripting (XSS) vulnerability in sidebar and table data that can result in Database fields aren't properly sanitized and allow code injection (Cross-Site Scripting). This attack appears to be exploitable via the payload needs to be stored in the database and the victim must see the db value in question. **CVE ID : CVE-2019-1000004**		
Kanboard					
Kanboard					
N/A	2019-02-04	4.3	app/Core/Paginator.php in Kanboard before 1.2.8 has XSS in pagination sorting. **CVE ID : CVE-2019-7324**	N/A	A-KAN-KANB-020419/123
Kentico					
kentico					
N/A	2019-02-08	4	** DISPUTED ** Kentico v10.0.42 allows Global Administrators to read the cleartext SMTP Password by navigating to the SMTP configuration page. NOTE: the vendor considers this a best-practice violation but not a vulnerability. The vendor plans to fix it at a future time. **CVE ID : CVE-2019-6242**	N/A	A-KEN-KENT-020419/124
kindsoft					
kindeditor					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-06	4.3	In KindEditor 4.1.11, the php/demo.php content1 parameter has a reflected Cross-site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-7543**	N/A	A-KIN-KIND-020419/125
Libarchive					
Libarchive					
N/A	2019-02-04	4.3	libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). This attack appears to be exploitable via the victim opening a specially crafted 7zip file. **CVE ID : CVE-2019-1000019**	N/A	A-LIB-LIBA-020419/126
N/A	2019-02-04	4.3	libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c, read_CE()/parse_rockridge() that can result in DoS by infinite loop. This attack	N/A	A-LIB-LIBA-020419/127

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			appears to be exploitable via the victim opening a specially crafted ISO9660 file. **CVE ID : CVE-2019-1000020**		
Libming					
Libming					
N/A	2019-02-07	6.8	The parseSWF_ACTIONRECORD function in util/parser.c in libming through 0.4.8 allows remote attackers to have unspecified impact via a crafted swf file that triggers a memory allocation failure, a different vulnerability than CVE-2018-7876. **CVE ID : CVE-2019-7581**	N/A	A-LIB-LIBM-020419/128
N/A	2019-02-07	6.8	The readBytes function in util/read.c in libming through 0.4.8 allows remote attackers to have unspecified impact via a crafted swf file that triggers a memory allocation failure. **CVE ID : CVE-2019-7582**	N/A	A-LIB-LIBM-020419/129
Libpng					
Libpng					
N/A	2019-02-04	2.6	png_image_free in png.c in libpng 1.6.36 has a use-after-free because png_image_free_function is called under png_safe_execute. **CVE ID : CVE-2019-7317**	N/A	A-LIB-LIBP-020419/130
libsdl					
simple_directmedia_layer					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in IMA_ADPCM_nibble in audio/SDL_wave.c. **CVE ID : CVE-2019-7572**	N/A	A-LIB-SIMP-020419/131
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (inside the wNumCoef loop). **CVE ID : CVE-2019-7573**	N/A	A-LIB-SIMP-020419/132
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in IMA_ADPCM_decode in audio/SDL_wave.c. **CVE ID : CVE-2019-7574**	N/A	A-LIB-SIMP-020419/133
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in MS_ADPCM_decode in audio/SDL_wave.c. **CVE ID : CVE-2019-7575**	N/A	A-LIB-SIMP-020419/134
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (outside the wNumCoef loop).	N/A	A-LIB-SIMP-020419/135

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7576		
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in SDL_LoadWAV_RW in audio/SDL_wave.c. **CVE ID : CVE-2019-7577**	N/A	A-LIB-SIMP-020419/136
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitIMA_ADPCM in audio/SDL_wave.c. **CVE ID : CVE-2019-7578**	N/A	A-LIB-SIMP-020419/137
N/A	2019-02-08	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in Blit1to4 in video/SDL_blit_1.c. **CVE ID : CVE-2019-7635**	N/A	A-LIB-SIMP-020419/138
N/A	2019-02-08	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in SDL_GetRGB in video/SDL_pixels.c. **CVE ID : CVE-2019-7636**	N/A	A-LIB-SIMP-020419/139
N/A	2019-02-08	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in SDL_FillRect in video/SDL_surface.c. **CVE ID : CVE-2019-7637**	N/A	A-LIB-SIMP-020419/140
N/A	2019-02-08	6.8	SDL (Simple DirectMedia	N/A	A-LIB-SIMP-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in Map1toN in video/SDL_pixels.c. **CVE ID : CVE-2019-7638**		020419/141
Libtiff					
Libtiff					
N/A	2019-02-09	4.3	An Invalid Address dereference was discovered in TIFFWriteDirectoryTagTransferfunction in libtiff/tif_dirwrite.c in LibTIFF 4.0.10, affecting the cpSeparateBufToContigBuf function in tiffcp.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. This is different from CVE-2018-12900. **CVE ID : CVE-2019-7663**	N/A	A-LIB-LIBT-020419/142
Linuxcontainers					
LXC					
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which		N/A	A-LIN-LXC-020419/143

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe. **CVE ID : CVE-2019-5736**		
Live555					
streaming_media					
N/A	2019-02-11	5	In Live555 0.95, a setup packet can cause a memory leak leading to DoS because, when there are multiple instances of a single field (username, realm, nonce, uri, or response), only the last instance can ever be freed. **CVE ID : CVE-2019-7732**	N/A	A-LIV-STRE-020419/144
N/A	2019-02-11	5	In Live555 0.95, there is a buffer overflow via a large integer in a Content-Length HTTP header because handleRequestBytes has an unrestricted memmove. **CVE ID : CVE-2019-7733**	N/A	A-LIV-STRE-020419/145
mapsvg					
mapsvg_lite					
N/A	2019-02-04	6.8	MapSVG MapSVG Lite version 3.2.3 contains a Cross Site Request Forgery (CSRF) vulnerability in REST endpoint /wp-admin/admin-ajax.php?action=mapsvg_save that can result in an attacker can modify post data,	N/A	A-MAP-MAPS-020419/146

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including embedding javascript. This attack appears to be exploitable via the victim must be logged in to WordPress as an admin, and click a link. This vulnerability appears to have been fixed in 3.3.0 and later. **CVE ID : CVE-2019-1000003**		
marlam					
mpop					
N/A	2019-02-13	5	In msmtp 1.8.2 and mpop 1.4.3, when tls_trust_file has its default configuration, certificate-verification results are not properly checked. **CVE ID : CVE-2019-8337**	https://marlam.de/msmtp/news/	A-MAR-MPOP-020419/147
msmtp					
N/A	2019-02-13	5	In msmtp 1.8.2 and mpop 1.4.3, when tls_trust_file has its default configuration, certificate-verification results are not properly checked. **CVE ID : CVE-2019-8337**	https://marlam.de/msmtp/news/	A-MAR-MSMT-020419/148
Mcafee					
epolicy_orchestrator					
N/A	2019-02-01	6.8	Cross-Site Request Forgery (CSRF) vulnerability in McAfee ePO (legacy) Cloud allows unauthenticated users to perform unintended ePO actions using an authenticated user's session via unspecified vectors.	https://kc.mcafee.com/corporate/index?page=content&id=SB10268	A-MCA-EPOL-020419/149

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3604		
true_key					
N/A	2019-02-13	2.1	Data Leakage Attacks vulnerability in Microsoft Windows client in McAfee True Key (TK) 3.1.9211.0 and earlier allows local users to expose confidential data via specially crafted malware. **CVE ID : CVE-2019-3610**	https://service.mcafee.com/webcenter/portal/cp/home/articleview?articleId=TS102889	A-MCA-TRUE-020419/150
Metinfo					
Metinfo					
N/A	2019-02-10	6.8	An issue was discovered in Metinfo 6.x. An attacker can leverage a race condition in the backend database backup function to execute arbitrary PHP code via admin/index.php?n=databack&c=index&a=dogetsql&tables=<?php and admin/databack/bakup_tables.php?2=file_put_contents URIs because app/system/databack/admin/index.class.php creates bakup_tables.php temporarily. **CVE ID : CVE-2019-7718**	N/A	A-MET-METI-020419/151
micco					
unlha32.dll					
N/A	2019-02-13	6.8	Untrusted search path vulnerability in the installer of UNLHA32.DLL (UNLHA32.DLL for Win32 Ver 2.67.1.2 and earlier) allows an attacker to	N/A	A-MIC-UNLH-020419/152

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2019-5911**		
unarj32.dll					
N/A	2019-02-13	6.8	Untrusted search path vulnerability in the installer of UNARJ32.DLL (UNARJ32.DLL for Win32 Ver 1.10.1.25 and earlier) allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2019-5912**	N/A	A-MIC-UNAR-020419/153
lhmelting					
N/A	2019-02-13	6.8	Untrusted search path vulnerability in the installer of LHMelting (LHMelting for Win32 Ver 1.65.3.6 and earlier) allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2019-5913**	N/A	A-MIC-LHME-020419/154
mpdf_project					
mpdf					
N/A	2019-02-04	6.8	mPDF version 7.1.7 and earlier contains a CWE-502: Deserialization of Untrusted Data vulnerability in getImage() method of Image/ImageProcessor class that can result in Arbitry code execution, file write, etc.. This attack appears to be	N/A	A-MPD-MPDF-020419/155

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable via attacker must host crafted image on victim server and trigger generation of pdf file with content <img src="phar://path/to/crafted/image">. This vulnerability appears to have been fixed in 7.1.8. **CVE ID : CVE-2019-1000005**		
Mywebsql					
Mywebsql					
N/A	2019-02-06	3.5	An issue was discovered in MyWebSQL 3.7. The Add User function of the User Manager pages has a Stored Cross-site Scripting (XSS) vulnerability in the User Name Field. **CVE ID : CVE-2019-7544**	N/A	A-MYW-MYWE-020419/156
N/A	2019-02-11	4.9	MyWebSQL 3.7 has a Cross-site request forgery (CSRF) vulnerability for deleting a database via the /?q=wrkfrm&type=databases URI. **CVE ID : CVE-2019-7730**	N/A	A-MYW-MYWE-020419/157
N/A	2019-02-11	7.5	MyWebSQL 3.7 has a remote code execution (RCE) vulnerability after an attacker writes shell code into the database, and executes the Backup Database function with a .php filename for the backup's archive file. **CVE ID : CVE-2019-7731**	N/A	A-MYW-MYWE-020419/158
Nasm					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
netwide_assembler					
N/A	2019-02-15	6.8	In Netwide Assembler (NASM) 2.14.02, there is a use-after-free in paste_tokens in asm/preproc.c. **CVE ID : CVE-2019-8343**	N/A	A-NAS-NETW-020419/159
nconsulting					
nc-cms					
N/A	2019-02-10	5	lib/NCCms.class.php in nc-cms 3.5 allows upload of .php files via the index.php?action=save name and editordata parameters. **CVE ID : CVE-2019-7721**	N/A	A-NCO-NC-C-020419/160
Netapp					
clustered_data_ontap					
N/A	2019-02-06	7.5	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted	N/A	A-NET-CLUS-020419/161

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header. **CVE ID : CVE-2019-3822**		
N/A	2019-02-06	5	libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to \`smtp_endofresp()\` isn't NUL terminated and contains no character ending the parsed number, and \`len\` is set to 5, then the \`strtol()\` call reads beyond the allocated buffer. The read contents will not be returned to the caller. **CVE ID : CVE-2019-3823**	N/A	A-NET-CLUS-020419/162
Nginx					
unit					
N/A	2019-02-07	7.5	NGINX Unit before 1.7.1 might allow an attacker to cause a heap-based buffer overflow in the router process with a specially crafted request. This may result in a denial of service (router process crash) or possibly have unspecified other impact.	N/A	A-NGI-UNIT-020419/163

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7401		
Nibbleblog					
Nibbleblog					
N/A	2019-02-10	7.5	Nibbleblog 4.0.5 allows eval injection by placing PHP code in the install.php username parameter and then making a content/private/shadow.php request. **CVE ID : CVE-2019-7719**	N/A	A-NIB-NIBB-020419/164
Opencontainers					
Runc					
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe. **CVE ID : CVE-2019-5736**	N/A	A-OPE-RUNC-020419/165
opt-net					
ng-netms					
N/A	2019-02-04	7.5	OPT/NET BV OPTOSS Next	N/A	A-OPT-NG-N-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Gen Network Management System (NG-NetMS) version v3.6-2 and earlier versions contains a SQL Injection vulnerability in Identified vulnerable parameters: id, id_access_type and id_attr_access that can result in a malicious attacker can include own SQL commands which database will execute. This attack appears to be exploitable via network connectivity. **CVE ID : CVE-2019-1000023**		020419/166
N/A	2019-02-04	4.3	OPT/NET BV NG-NetMS version v3.6-2 and earlier versions contains a Cross Site Scripting (XSS) vulnerability in /js/libs/jstree/demo/filebrowser/index.php page. The "id" and "operation" GET parameters can be used to inject arbitrary JavaScript which is returned in the page's response that can result in Cross-site scripting.This attack appear to be exploitable via network connectivity. **CVE ID : CVE-2019-1000024**	N/A	A-OPT-NG-N-020419/167
osstech					
openam					
N/A	2019-02-13	5.8	Open redirect vulnerability in OpenAM (Open Source Edition) 13.0 allows remote attackers to redirect users to arbitrary web sites and	N/A	A-OSS-OPEN-020419/168

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conduct phishing attacks via a specially crafted page. **CVE ID : CVE-2019-5915**		
Pbootcms					
Pbootcms					
N/A	2019-02-07	5.8	A CSRF vulnerability was found in PbootCMS v1.3.6 that can delete users via an admin.php/User/del/ucode/ URI. **CVE ID : CVE-2019-7570**	N/A	A-PBO-PBOO-020419/169
Phpipam					
Phpipam					
N/A	2019-02-04	4.3	phpIPAM version 1.3.2 and earlier contains a Cross Site Scripting (XSS) vulnerability in subnet-scan-telnet.php that can result in executing code in victims browser. This attack appears to be exploitable via victim visits link crafted by an attacker. This vulnerability appears to have been fixed in 1.4. **CVE ID : CVE-2019-1000010**	N/A	A-PHP-PHPI-020419/170
phpmywind					
phpmywind					
N/A	2019-02-05	4.3	An issue was discovered in PHPMyWind 5.5. The GetQQ function in include/func.class.php allows XSS via the cfg&#95;qqcode parameter. This can be exploited via CSRF.	N/A	A-PHP-PHPM-020419/171

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7402		
N/A	2019-02-05	5.5	An issue was discovered in PHPMyWind 5.5. It allows remote attackers to delete arbitrary folders via an admin/database_backup.php?action=import&dopost=deldir&tbname=../ URI. **CVE ID : CVE-2019-7403**	N/A	A-PHP-PHPM-020419/172
Pizzashack					
Rssh					
N/A	2019-02-04	4.6	rssh version 2.3.4 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in allowscp permission that can result in Local command execution. This attack appear to be exploitable via An authorized SSH user with the allowscp permission. **CVE ID : CVE-2019-1000018**	N/A	A-PIZ-RSSH-020419/173
N/A	2019-02-06	7.5	Insufficient sanitization of arguments passed to rsync can bypass the restrictions imposed by rssh, a restricted shell that should restrict users to perform only rsync operations, resulting in the execution of arbitrary shell commands. **CVE ID : CVE-2019-3463**	N/A	A-PIZ-RSSH-020419/174
N/A	2019-02-06	7.5	Insufficient sanitization of environment variables passed	N/A	A-PIZ-RSSH-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to rsync can bypass the restrictions imposed by rssh, a restricted shell that should restrict users to perform only rsync operations, resulting in the execution of arbitrary shell commands. **CVE ID : CVE-2019-3464**		020419/175
pmd_project					
pmd					
N/A	2019-02-11	6.8	PMD 5.8.1 and earlier processes XML external entities in ruleset files it parses as part of the analysis process, allowing attackers tampering it (either by direct modification or MITM attacks when using remote rulesets) to perform information disclosure, denial of service, or request forgery attacks. (PMD 6.x is unaffected because of a 2017-09-15 change.) **CVE ID : CVE-2019-7722**	N/A	A-PMD-PMD-020419/176
Pocoo					
Jinja2					
N/A	2019-02-15	7.5	An issue was discovered in Jinja2 2.10. The from_string function is prone to Server Side Template Injection (SSTI) where it takes the "source" parameter as a template object, renders it, and then returns it. The attacker can exploit it with {{INJECTION COMMANDS}} in a URI.	N/A	A-POC-JINJ-020419/177

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8341		
rdflib_project					
rdflib					
N/A	2019-02-08	7.5	The Debian python-rdflib-tools 4.2.2-1 package for RDFLib 4.2.2 has CLI tools that can load Python modules from the current working directory, allowing code injection, because "python -m" looks in this directory, as demonstrated by rdf2dot. This issue is specific to use of the debian/scripts directory. **CVE ID : CVE-2019-7653**	N/A	A-RDF-RDFL-020419/178
Redhat					
Openshift					
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.	N/A	A-RED-OPEN-020419/179

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5736		
openshift_container_platform					
N/A	2019-02-06	4.3	A cross-site request forgery vulnerability exists in Jenkins Git Plugin 3.9.1 and earlier in src/main/java/hudson/plugins/git/GitTagAction.java that allows attackers to create a Git tag in a workspace and attach corresponding metadata to a build record. **CVE ID : CVE-2019-1003010**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1095	A-RED-OPEN-020419/180
N/A	2019-02-06	5.5	An information exposure and denial of service vulnerability exists in Jenkins Token Macro Plugin 2.5 and earlier in src/main/java/org/jenkinsci/plugins/tokenmacro/Parser.java, src/main/java/org/jenkinsci/plugins/tokenmacro/TokenMacro.java, src/main/java/org/jenkinsci/plugins/tokenmacro/impl/AbstractChangesSinceMacro.java, src/main/java/org/jenkinsci/plugins/tokenmacro/impl/ChangesSinceLastBuildMacro.java, src/main/java/org/jenkinsci/plugins/tokenmacro/impl/ProjectUrlMacro.java that allows attackers with the ability to control token macro input (such as SCM changelogs) to define recursive input that results in unexpected macro	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1102	A-RED-OPEN-020419/181

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			evaluation. **CVE ID : CVE-2019-1003011**		
N/A	2019-02-06	4.3	A data modification vulnerability exists in Jenkins Blue Ocean Plugins 1.10.1 and earlier in blueocean-core-js/src/js/bundleStartup.js, blueocean-core-js/src/js/fetch.ts, blueocean-core-js/src/js/i18n/i18n.js, blueocean-core-js/src/js/urlconfig.js, blueocean-rest/src/main/java/io/jenkins/blueocean/rest/APICrumbExclusion.java, blueocean-web/src/main/java/io/jenkins/blueocean/BlueOceanUI.java, blueocean-web/src/main/resources/io/jenkins/blueocean/BlueOceanUI/index.jelly that allows attackers to bypass all cross-site request forgery protection in Blue Ocean API. **CVE ID : CVE-2019-1003012**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1201	A-RED-OPEN-020419/182
N/A	2019-02-06	3.5	An cross-site scripting vulnerability exists in Jenkins Blue Ocean Plugins 1.10.1 and earlier in blueocean-commons/src/main/java/io/jenkins/blueocean/commons/stapler/Export.java, blueocean-commons/src/main/java/io/jenkins/blueocean/commons/stapler/export/ExportConfig.java, blueocean-	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1204	A-RED-OPEN-020419/183

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commons/src/main/java/io/jenkins/blueocean/commons/stapler/export/JSONDataWriter.java, blueocean-rest-impl/src/main/java/io/jenkins/blueocean/service/embedded/UserStatePreloader.java, blueocean-web/src/main/resources/io/jenkins/blueocean/PageStatePreloadDecorator/header.jelly that allows attackers with permission to edit a user's description in Jenkins to have Blue Ocean render arbitrary HTML when using it as that user. **CVE ID : CVE-2019-1003013**		
N/A	2019-02-06	3.5	An cross-site scripting vulnerability exists in Jenkins Config File Provider Plugin 3.4.1 and earlier in src/main/resources/lib/configfiles/configfiles.jelly that allows attackers with permission to define shared configuration files to execute arbitrary JavaScript when a user attempts to delete the shared configuration file. **CVE ID : CVE-2019-1003014**	https://jenkins.io/security/advisory/2019-01-28/#SECURITY-1253	A-RED-OPEN-020419/184
N/A	2019-02-05	5	The kube-rbac-proxy container before version 0.4.1 as used in Red Hat OpenShift Container Platform does not honor TLS configurations, allowing for use of insecure	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3818	A-RED-OPEN-020419/185

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ciphers and TLS 1.0. An attacker could target traffic sent over a TLS connection with a weak configuration and potentially break the encryption. **CVE ID : CVE-2019-3818**		
pagure					
N/A	2019-02-07	4.3	Pagure 5.2 leaks API keys by e-mailing them to users. Few e-mail servers validate TLS certificates, so it is easy for man-in-the-middle attackers to read these e-mails and gain access to Pagure on behalf of other users. This issue is found in the API token expiration reminder cron job in files/api_key_expire_mail.py; disabling that job is also a viable solution. (E-mailing a substring of the API key was an attempted, but rejected, solution.) **CVE ID : CVE-2019-7628**	N/A	A-RED-PAGU-020419/186
SAP					
landscape_management					
N/A	2019-02-15	7.5	Under certain circumstances, SAP HANA Extended Application Services, advanced model (XS advanced) does not perform authentication checks properly for XS advanced platform and business users. Fixed in 1.0.97 to 1.0.99 (running on SAP HANA 1 or	N/A	A-SAP-LAND-020419/187

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SAP HANA 2 SPS0 (second S stands for stack)). **CVE ID : CVE-2019-0261**		
advanced_business_application_programming_platform_kernel					
N/A	2019-02-15	5.5	SAP NetWeaver AS ABAP Platform, Krnl64nuc 7.74, krnl64UC 7.73, 7.74, Kernel 7.73, 7.74, 7.75, fails to validate type of installation for an ABAP Server system correctly. That behavior may lead to situation, where business user achieves access to the full SAP Menu, that is 'Easy Access Menu'. The situation can be misused by any user to leverage privileges to business functionality. **CVE ID : CVE-2019-0255**	N/A	A-SAP-ADVA-020419/188
N/A	2019-02-15	4	SLD Registration of ABAP Platform allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. Fixed in versions KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT,KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49,KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73 KERNEL from 7.21 to 7.22, 7.45, 7.49, 7.53, 7.73, 7.75. **CVE ID : CVE-2019-0265**	N/A	A-SAP-ADVA-020419/189
advanced_business_application_programming_platform_krnl64nuc					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-15	5.5	SAP NetWeaver AS ABAP Platform, Krnl64nuc 7.74, krnl64UC 7.73, 7.74, Kernel 7.73, 7.74, 7.75, fails to validate type of installation for an ABAP Server system correctly. That behavior may lead to situation, where business user achieves access to the full SAP Menu, that is 'Easy Access Menu'. The situation can be misused by any user to leverage privileges to business functionality. **CVE ID : CVE-2019-0255**	N/A	A-SAP-ADVA-020419/190
N/A	2019-02-15	4	SLD Registration of ABAP Platform allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. Fixed in versions KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT,KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49,KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73 KERNEL from 7.21 to 7.22, 7.45, 7.49, 7.53, 7.73, 7.75. **CVE ID : CVE-2019-0265**	N/A	A-SAP-ADVA-020419/191
advanced_business_application_programming_platform_krnl64uc					
N/A	2019-02-15	5.5	SAP NetWeaver AS ABAP Platform, Krnl64nuc 7.74, krnl64UC 7.73, 7.74, Kernel 7.73, 7.74, 7.75, fails to validate type of installation for	N/A	A-SAP-ADVA-020419/192

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an ABAP Server system correctly. That behavior may lead to situation, where business user achieves access to the full SAP Menu, that is 'Easy Access Menu'. The situation can be misused by any user to leverage privileges to business functionality. **CVE ID : CVE-2019-0255**		
N/A	2019-02-15	4	SLD Registration of ABAP Platform allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. Fixed in versions KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT,KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49,KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73 KERNEL from 7.21 to 7.22, 7.45, 7.49, 7.53, 7.73, 7.75. **CVE ID : CVE-2019-0265**	N/A	A-SAP-ADVA-020419/193
business_one					
N/A	2019-02-15	2.1	Under certain conditions SAP Business One Mobile Android App, version 1.2.12, allows an attacker to access information which would otherwise be restricted. **CVE ID : CVE-2019-0256**	N/A	A-SAP-BUSI-020419/194
netweaver_abap					
N/A	2019-02-15	6.5	Customizing functionality of	N/A	A-SAP-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SAP NetWeaver AS ABAP Platform (fixed in versions from 7.0 to 7.02, from 7.10 to 7.11, 7.30, 7.31, 7.40, from 7.50 to 7.53, from 7.74 to 7.75) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2019-0257**		NETW-020419/195
disclosure_management					
N/A	2019-02-15	6.5	SAP Disclosure Management, version 10.01, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2019-0258**	N/A	A-SAP-DISC-020419/196
businessobjects_bi_platform					
N/A	2019-02-15	3.5	SAP WebIntelligence BILaunchPad, versions 4.10, 4.20, does not sufficiently encode user-controlled inputs in generated HTML reports, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-0262**	N/A	A-SAP-BUSI-020419/197
advanced_business_application_programming_platform_krnl32nuc					
N/A	2019-02-15	4	SLD Registration of ABAP Platform allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. Fixed in versions KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT,KRNL32UC 7.21,	N/A	A-SAP-ADVA-020419/198

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49,KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73 KERNEL from 7.21 to 7.22, 7.45, 7.49, 7.53, 7.73, 7.75. **CVE ID : CVE-2019-0265**		
advanced_business_application_programming_platform_krnl32uc					
N/A	2019-02-15	4	SLD Registration of ABAP Platform allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. Fixed in versions KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT,KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49,KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49. 7.73 KERNEL from 7.21 to 7.22, 7.45, 7.49, 7.53, 7.73, 7.75. **CVE ID : CVE-2019-0265**	N/A	A-SAP-ADVA-020419/199
hana_extended_application_services					
N/A	2019-02-15	5	Under certain conditions SAP HANA Extended Application Services, version 1.0, advanced model (XS advanced) writes credentials of platform users to a trace file of the SAP HANA system. Even though this trace file is protected from unauthorized access, the risk of leaking information is	N/A	A-SAP-HANA-020419/200

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			increased. **CVE ID : CVE-2019-0266**		
manufacturing_integration_and_intelligence					
N/A	2019-02-15	6.8	SAP Manufacturing Integration and Intelligence, versions 15.0, 15.1 and 15.2, (Illuminator Servlet) currently does not provide Anti-XSRF tokens. This might lead to XSRF attacks in case the data is being posted to the Servlet from an external application. **CVE ID : CVE-2019-0267**	N/A	A-SAP-MANU-020419/201
Businessobjects					
N/A	2019-02-15	4.3	The Fiori Launchpad of SAP BusinessObjects, before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-0251**	N/A	A-SAP-BUSI-020419/202
N/A	2019-02-15	7.5	SAP BusinessObjects, versions 4.2 and 4.3, (Visual Difference) allows an attacker to upload any file (including script files) without proper file format validation. **CVE ID : CVE-2019-0259**	N/A	A-SAP-BUSI-020419/203
schoolcms					
schoolcms					
N/A	2019-02-13	4.3	An issue was discovered in SchoolCMS 2.3.1. There is an XSS vulnerability via index.php?a=Index&c=Channel	N/A	A-SCH-SCHO-020419/204

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			&m=Home&viewid=[XSS]. **CVE ID : CVE-2019-8334**		
N/A	2019-02-13	4.3	An issue was discovered in SchoolCMS 2.3.1. There is an XSS vulnerability via index.php?a=Index&c=Channel&m=Home&id=[XSS]. **CVE ID : CVE-2019-8335**	N/A	A-SCH-SCHO-020419/205
sound_exchange_project					
sound_exchange					
N/A	2019-02-15	4.3	An issue was discovered in SoX 14.4.2. lsx_make_lpf in effect_i_dsp.c has an integer overflow on the result of multiplication fed into malloc. When the buffer is allocated, it is smaller than expected, leading to a heap-based buffer overflow. **CVE ID : CVE-2019-8354**	N/A	A-SOU-SOUN-020419/206
N/A	2019-02-15	4.3	An issue was discovered in SoX 14.4.2. In xmalloc.h, there is an integer overflow on the result of multiplication fed into the lsx_valloc macro that wraps malloc. When the buffer is allocated, it is smaller than expected, leading to a heap-based buffer overflow in channels_start in remix.c. **CVE ID : CVE-2019-8355**	N/A	A-SOU-SOUN-020419/207
N/A	2019-02-15	4.3	An issue was discovered in SoX 14.4.2. One of the arguments to bitrv2 in fft4g.c is not guarded, such that it can lead	N/A	A-SOU-SOUN-020419/208

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to write access outside of the statically declared array, aka a stack-based buffer overflow. **CVE ID : CVE-2019-8356**		
N/A	2019-02-15	4.3	An issue was discovered in SoX 14.4.2. lsx_make_lpf in effect_i_dsp.c allows a NULL pointer dereference. **CVE ID : CVE-2019-8357**	N/A	A-SOU-SOUN-020419/209
spice_project					
spice					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	A-SPI-SPIC-020419/210
Sqlalchemy					
Sqlalchemy					
N/A	2019-02-06	6.8	SQLAlchemy 1.2.17 has SQL Injection when the group_by parameter can be controlled. **CVE ID : CVE-2019-7548**	N/A	A-SQL-SQLA-020419/211
taoensso					
sente					
N/A	2019-02-04	6.8	Taoensso Sente version Prior to version 1.14.0 contains a Cross Site Request Forgery (CSRF) vulnerability in WebSocket handshake	N/A	A-TAO-SENT-020419/212

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			endpoint that can result in CSRF attack, possible leak of anti-CSRF token. This attack appears to be exploitable via malicious request against WebSocket handshake endpoint. This vulnerability appears to have been fixed in 1.14.0 and later. **CVE ID : CVE-2019-1000022**		
taogogo					
taocms					
N/A	2019-02-10	7.5	taocms through 2014-05-24 allows eval injection by placing PHP code in the install.php db_name parameter and then making a config.php request. **CVE ID : CVE-2019-7720**	N/A	A-TAO-TAOC-020419/213
Teampass					
Teampass					
N/A	2019-02-04	5	TeamPass version 2.1.27 and earlier contains a Storing Passwords in a Recoverable Format vulnerability in Shared password vaults that can result in all shared passwords are recoverable server side. This attack appears to be exploitable via any vulnerability that can bypass authentication or role assignment and can lead to shared password leakage. **CVE ID : CVE-2019-1000001**	N/A	A-TEA-TEAM-020419/214
Tenable					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Nessus					
N/A	2019-02-11	3.5	Nessus versions 8.2.1 and earlier were found to contain a stored XSS vulnerability due to improper validation of user-supplied input. An authenticated, remote attacker could potentially exploit this vulnerability via a specially crafted request to execute arbitrary script code in a user's browser session. Tenable has released Nessus 8.2.2 to address this issue. **CVE ID : CVE-2019-3923**	https://www.tenable.com/security/tns-2019-01	A-TEN-NESS-020419/215
Thinkcmf					
Thinkcmf					
N/A	2019-02-07	6.5	ThinkCMF 5.0.190111 allows remote attackers to execute arbitrary PHP code via the portal/admin_category/addpost.html alias parameter because the mishandling of a single quote character allows data/conf/route.php injection. **CVE ID : CVE-2019-7580**	N/A	A-THI-THIN-020419/216
topnew					
sidu					
N/A	2019-02-06	4.3	An issue was discovered in SIDU 6.0. The dbs parameter of the conn.php page has a reflected Cross-site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-7546**	N/A	A-TOP-SIDU-020419/217
N/A	2019-02-06	3.5	An issue was discovered in	N/A	A-TOP-SIDU-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIDU 6.0. Because the database name is not strictly filtered, the attacker can insert a name containing an XSS Payload, leading to stored XSS. **CVE ID : CVE-2019-7547**		020419/218
verydows					
verydows					
N/A	2019-02-11	6.8	A CSRF vulnerability was found in Verydows v2.0 that can add an admin account via index.php?m=backend&c=admin&a=add&step=submit. **CVE ID : CVE-2019-7737**	N/A	A-VER-VERY-020419/219
N/A	2019-02-12	4.3	Verydows 2.0 has XSS via the index.php?m=api&c=stats&a=count referrer parameter. **CVE ID : CVE-2019-7753**	N/A	A-VER-VERY-020419/220
wdoyo					
doyo					
N/A	2019-02-07	6.8	An issue was discovered in DOYO (aka doyocms) 2.3(20140425 update). There is a CSRF vulnerability that can add a super administrator account via admin.php?c=a_adminuser&a=add&run=1. **CVE ID : CVE-2019-7569**	N/A	A-WDO-DOYO-020419/221
webassembly					
binaryen					
N/A	2019-02-09	7.1	An assertion failure was discovered in wasm::WasmBinaryBuilder::ge	N/A	A-WEB-BINA-020419/222

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tType() in wasm-binary.cpp in Binaryen 1.38.22. This allows remote attackers to cause a denial of service (failed assertion and crash) via a crafted wasm file. **CVE ID : CVE-2019-7662**		
N/A	2019-02-10	4.3	A heap-based buffer over-read was discovered in wasm::WasmBinaryBuilder::visitCall in wasm-binary.cpp in Binaryen 1.38.22. A crafted wasm input can cause a segmentation fault, leading to denial-of-service, as demonstrated by wasm-merge. **CVE ID : CVE-2019-7700**	N/A	A-WEB-BINA-020419/223
N/A	2019-02-10	4.3	A heap-based buffer over-read was discovered in wasm::SExpressionParser::skipWhitespace() in wasm-s-parser.cpp in Binaryen 1.38.22. A crafted wasm input can cause a segmentation fault, leading to denial-of-service, as demonstrated by wasm2js. **CVE ID : CVE-2019-7701**	N/A	A-WEB-BINA-020419/224
N/A	2019-02-10	4.3	A NULL pointer dereference was discovered in wasm::SExpressionWasmBuilder::parseExpression in wasm-s-parser.cpp in Binaryen 1.38.22. A crafted wasm input can cause a segmentation fault, leading to denial-of-service, as	N/A	A-WEB-BINA-020419/225

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			demonstrated by wasm-as. **CVE ID : CVE-2019-7702**		
N/A	2019-02-10	4.3	In Binaryen 1.38.22, there is a use-after-free problem in wasm::WasmBinaryBuilder::visitCall in wasm-binary.cpp. Remote attackers could leverage this vulnerability to cause a denial-of-service via a wasm file, as demonstrated by wasm-merge. **CVE ID : CVE-2019-7703**	N/A	A-WEB-BINA-020419/226
N/A	2019-02-10	4.3	wasm::WasmBinaryBuilder::readUserSection in wasm-binary.cpp in Binaryen 1.38.22 triggers an attempt at excessive memory allocation, as demonstrated by wasm-merge and wasm-opt. **CVE ID : CVE-2019-7704**	N/A	A-WEB-BINA-020419/227
We-con					
levistudiou					
N/A	2019-02-12	6.8	Multiple stack-based buffer overflow vulnerabilities in WECON LeviStudioU version 1.8.56 and prior may be exploited when parsing strings within project files. The process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage these vulnerabilities to execute code under the context of the current process.	N/A	A-WE--LEVI-020419/228

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mat Powell, Ziad Badawi, and Natnael Samson working with Trend Micro's Zero Day Initiative, reported these vulnerabilities to NCCIC. **CVE ID : CVE-2019-6537**		
N/A	2019-02-12	9.3	Several heap-based buffer overflow vulnerabilities in WECON LeviStudioU version 1.8.56 and prior have been identified, which may allow arbitrary code execution. Mat Powell, Ziad Badawi, and Natnael Samson working with Trend Micro's Zero Day Initiative, reported these vulnerabilities to NCCIC. **CVE ID : CVE-2019-6539**	N/A	A-WE--LEVI-020419/229
N/A	2019-02-12	6.8	A memory corruption vulnerability has been identified in WECON LeviStudioU version 1.8.56 and prior, which may allow arbitrary code execution. Mat Powell, Ziad Badawi, and Natnael Samson working with Trend Micro's Zero Day Initiative, reported these vulnerabilities to NCCIC. **CVE ID : CVE-2019-6541**	N/A	A-WE--LEVI-020419/230
Yokogawa					
centum_vp					
N/A	2019-02-13	10	License Manager Service of YOKOGAWA products (CENTUM VP (R5.01.00 - R6.06.00), CENTUM VP Entry	N/A	A-YOK-CENT-020419/231

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Class (R5.01.00 - R6.06.00), ProSafe-RS (R3.01.00 - R4.04.00), PRM (R4.01.00 - R4.02.00), B/M9000 VP(R7.01.01 - R8.02.03)) allows remote attackers to bypass access restriction to send malicious files to the PC where License Manager Service runs via unspecified vectors. **CVE ID : CVE-2019-5909**		
zevenet					
zen_load_balancer					
N/A	2019-02-01	9	Zen Load Balancer 3.10.1 allows remote authenticated admin users to execute arbitrary commands as root via shell metacharacters in the index.cgi?action=View_Cert certname parameter. **CVE ID : CVE-2019-7301**	N/A	A-ZEV-ZEN_-020419/232
Zoneminder					
Zoneminder					
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, as multiple views under web/skins/classic/views insecurely utilize $_REQUEST['PHP_SELF'], without applying any proper filtration. **CVE ID : CVE-2019-7325**	N/A	A-ZON-ZONE-020419/233
N/A	2019-02-04	4.3	Self - Stored Cross Site	N/A	A-ZON-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'Host' parameter value in the view console (console.php) because proper filtration is omitted. This relates to the index.php?view=monitor Host Name field. **CVE ID : CVE-2019-7326**		ZONE-020419/234
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'scale' parameter value in the view frame (frame.php) because proper filtration is omitted. **CVE ID : CVE-2019-7327**	N/A	A-ZON-ZONE-020419/235
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'scale' parameter value in the view frame (frame.php) via /js/frame.js.php because proper filtration is omitted. **CVE ID : CVE-2019-7328**	N/A	A-ZON-ZONE-020419/236
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, as the form action on multiple views	N/A	A-ZON-ZONE-020419/237

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			utilizes $_SERVER['PHP_SELF'] insecurely, mishandling any arbitrary input appended to the webroot URL, without any proper filtration, leading to XSS. **CVE ID : CVE-2019-7329**		
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'show' parameter value in the view frame (frame.php) because proper filtration is omitted. **CVE ID : CVE-2019-7330**	N/A	A-ZON-ZONE-020419/238
N/A	2019-02-04	4.3	Self - Stored Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3 while editing an existing monitor field named "signal check color" (monitor.php). There exists no input validation or output filtration, leaving it vulnerable to HTML Injection and an XSS attack. **CVE ID : CVE-2019-7331**	N/A	A-ZON-ZONE-020419/239
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'eid' (aka Event ID) parameter value in the view download (download.php) because proper filtration is	N/A	A-ZON-ZONE-020419/240

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			omitted. **CVE ID : CVE-2019-7332**		
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'Exportfile' parameter value in the view download (download.php) because proper filtration is omitted. **CVE ID : CVE-2019-7333**	N/A	A-ZON-ZONE-020419/241
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'Exportfile' parameter value in the view export (export.php) because proper filtration is omitted. **CVE ID : CVE-2019-7334**	N/A	A-ZON-ZONE-020419/242
N/A	2019-02-04	4.3	Self - Stored XSS exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code in the view 'log' as it insecurely prints the 'Log Message' value on the web page without applying any proper filtration. This relates to the view=logs value. **CVE ID : CVE-2019-7335**	N/A	A-ZON-ZONE-020419/243
N/A	2019-02-04	4.3	Self - Stored Cross Site Scripting (XSS) exists in	N/A	A-ZON-ZONE-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZoneMinder through 1.32.3, as the view _monitor_filters.php contains takes in input from the user and saves it into the session, and retrieves it later (insecurely). The values of the MonitorName and Source parameters are being displayed without any output filtration being applied. This relates to the view=cycle value. **CVE ID : CVE-2019-7336**		020419/244
N/A	2019-02-04	3.5	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3 as the view 'events' (events.php) insecurely displays the limit parameter value, without applying any proper output filtration. This issue exists because of the function sortHeader() in functions.php, which insecurely returns the value of the limit query string parameter without applying any filtration. **CVE ID : CVE-2019-7337**	N/A	A-ZON-ZONE-020419/245
N/A	2019-02-04	4.3	Self - Stored XSS exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code in the view 'group' as it insecurely prints the 'Group Name' value on the web page without applying any proper filtration. **CVE ID : CVE-2019-7338**	N/A	A-ZON-ZONE-020419/246

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-04	4.3	POST - Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'level' parameter value in the view log (log.php) because proper filtration is omitted. **CVE ID : CVE-2019-7339**	N/A	A-ZON-ZONE-020419/247
N/A	2019-02-04	4.3	POST - Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'filter[Query][terms][0][val]' parameter value in the view filter (filter.php) because proper filtration is omitted. **CVE ID : CVE-2019-7340**	N/A	A-ZON-ZONE-020419/248
N/A	2019-02-04	4.3	Reflected - Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'newMonitor[LinkedMonitors]' parameter value in the view monitor (monitor.php) because proper filtration is omitted. **CVE ID : CVE-2019-7341**	N/A	A-ZON-ZONE-020419/249
N/A	2019-02-04	4.3	POST - Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or	N/A	A-ZON-ZONE-020419/250

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code via a vulnerable 'filter[AutoExecuteCmd]' parameter value in the view filter (filter.php) because proper filtration is omitted. **CVE ID : CVE-2019-7342**		
N/A	2019-02-04	4.3	Reflected - Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'newMonitor[Method]' parameter value in the view monitor (monitor.php) because proper filtration is omitted. **CVE ID : CVE-2019-7343**	N/A	A-ZON-ZONE-020419/251
N/A	2019-02-04	4.3	Reflected XSS exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code in the view 'filter' as it insecurely prints the 'filter[Name]' (aka Filter name) value on the web page without applying any proper filtration. **CVE ID : CVE-2019-7344**	N/A	A-ZON-ZONE-020419/252
N/A	2019-02-04	3.5	Self - Stored Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, as the view 'options' (options.php) does no input validation for the WEB_TITLE, HOME_URL, HOME_CONTENT, or WEB_CONSOLE_BANNER	N/A	A-ZON-ZONE-020419/253

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			value, allowing an attacker to execute HTML or JavaScript code. This relates to functions.php. **CVE ID : CVE-2019-7345**		
N/A	2019-02-04	6.8	A CSRF check issue exists in ZoneMinder through 1.32.3 as whenever a CSRF check fails, a callback function is called displaying a "Try again" button, which allows resending the failed request, making the CSRF attack successful. **CVE ID : CVE-2019-7346**	N/A	A-ZON-ZONE-020419/254
N/A	2019-02-04	6	A Time-of-check Time-of-use (TOCTOU) Race Condition exists in ZoneMinder through 1.32.3 as a session remains active for an authenticated user even after deletion from the users table. This allows a nonexistent user to access and modify records (add/delete Monitors, Users, etc.). **CVE ID : CVE-2019-7347**	N/A	A-ZON-ZONE-020419/255
N/A	2019-02-04	4.3	Self - Stored Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'username' parameter value in the view user (user.php) because proper filtration is omitted. **CVE ID : CVE-2019-7348**	N/A	A-ZON-ZONE-020419/256

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-04	4.3	Reflected Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, allowing an attacker to execute HTML or JavaScript code via a vulnerable 'newMonitor[V4LCapturesPerFrame]' parameter value in the view monitor (monitor.php) because proper filtration is omitted. **CVE ID : CVE-2019-7349**	N/A	A-ZON-ZONE-020419/257
N/A	2019-02-04	4.9	Session fixation exists in ZoneMinder through 1.32.3, as an attacker can fixate his own session cookies to the next logged-in user, thereby hijacking the victim's account. This occurs because a set of multiple cookies (between 3 and 5) is being generated when a user successfully logs in, and these sets overlap for successive logins. **CVE ID : CVE-2019-7350**	N/A	A-ZON-ZONE-020419/258
N/A	2019-02-04	4.3	Log Injection exists in ZoneMinder through 1.32.3, as an attacker can entice the victim to visit a specially crafted link, which in turn will inject a custom Log message provided by the attacker in the 'log' view page, as demonstrated by the message=User%20'admin'%20Logged%20in value. **CVE ID : CVE-2019-7351**	N/A	A-ZON-ZONE-020419/259

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-04	4.3	Self - Stored Cross Site Scripting (XSS) exists in ZoneMinder through 1.32.3, as the view 'state' (aka Run State) (state.php) does no input validation to the value supplied to the 'New State' (aka newState) field, allowing an attacker to execute HTML or JavaScript code. **CVE ID : CVE-2019-7352**	N/A	A-ZON-ZONE-020419/260
OS					
BD					
facslyric					
N/A	2019-02-06	4.6	BD FACSLyric Research Use Only, Windows 10 Professional Operating System, U.S. and Malaysian Releases, between November 2017 and November 2018 and BD FACSLyric IVD Windows 10 Professional Operating System US release does not properly enforce user access control to privileged accounts, which may allow for unauthorized access to administrative level functions. **CVE ID : CVE-2019-6517**	N/A	O-BD-FACS-020419/261
facslyric_ivd					
N/A	2019-02-06	4.6	BD FACSLyric Research Use Only, Windows 10 Professional Operating System, U.S. and Malaysian Releases, between November 2017 and November 2018 and	N/A	O-BD-FACS-020419/262

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BD FACSLyric IVD Windows 10 Professional Operating System US release does not properly enforce user access control to privileged accounts, which may allow for unauthorized access to administrative level functions. **CVE ID : CVE-2019-6517**		
Canonical					
ubuntu_linux					
N/A	2019-02-04	4.3	libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). This attack appears to be exploitable via the victim opening a specially crafted 7zip file. **CVE ID : CVE-2019-1000019**	N/A	O-CAN-UBUN-020419/263
N/A	2019-02-04	4.3	libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c,	N/A	O-CAN-UBUN-020419/264

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read_CE()/parse_rockridge() that can result in DoS by infinite loop. This attack appears to be exploitable via the victim opening a specially crafted ISO9660 file. **CVE ID : CVE-2019-1000020**		
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	O-CAN-UBUN-020419/265
N/A	2019-02-06	7.5	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted	N/A	O-CAN-UBUN-020419/266

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header. **CVE ID : CVE-2019-3822**		
N/A	2019-02-06	5	libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to \`smtp_endofresp()\` isn't NUL terminated and contains no character ending the parsed number, and \`len\` is set to 5, then the \`strtol()\` call reads beyond the allocated buffer. The read contents will not be returned to the caller. **CVE ID : CVE-2019-3823**	N/A	O-CAN-UBUN-020419/267
N/A	2019-02-06	6.9	A vulnerability was discovered in gdm before 3.31.4. When timed login is enabled in configuration, an attacker could bypass the lock screen by selecting the timed login user and waiting for the timer to expire, at which time they would gain access to the logged-in user's session. **CVE ID : CVE-2019-3825**	N/A	O-CAN-UBUN-020419/268

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-11	5	Django 1.11.x before 1.11.19, 2.0.x before 2.0.11, and 2.1.x before 2.1.6 allows Uncontrolled Memory Consumption via a malicious attacker-supplied value to the django.utils.numberformat.format() function. **CVE ID : CVE-2019-6975**	N/A	O-CAN-UBUN-020419/269
N/A	2019-02-02	6.8	In Poppler 0.73.0, a heap-based buffer over-read (due to an integer signedness error in the XRef::getEntry function in XRef.cc) allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document, as demonstrated by pdftocairo. **CVE ID : CVE-2019-7310**	N/A	O-CAN-UBUN-020419/270
N/A	2019-02-09	4.3	An Invalid Address dereference was discovered in TIFFWriteDirectoryTagTransferfunction in libtiff/tif_dirwrite.c in LibTIFF 4.0.10, affecting the cpSeparateBufToContigBuf function in tiffcp.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. This is different from CVE-2018-12900. **CVE ID : CVE-2019-7663**	N/A	O-CAN-UBUN-020419/271
Cisco					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
unified_intelligence_center					
N/A	2019-02-07	4.3	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of an affected system. The vulnerability is due to insufficient input validation of a user-supplied value. An attacker could exploit this vulnerability by convincing a user to click a specific link. A successful exploit could allow the attacker to submit arbitrary requests to the affected system via a web browser with the privileges of the user. **CVE ID : CVE-2019-1670**	N/A	O-CIS-UNIF-020419/272
Debian					
debian_linux					
N/A	2019-02-04	4.6	rssh version 2.3.4 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in allowscp permission that can result in Local command execution. This attack appear to be exploitable via An authorized SSH user with the allowscp permission.	N/A	O-DEB-DEBI-020419/273

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1000018		
N/A	2019-02-04	4.3	libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). This attack appears to be exploitable via the victim opening a specially crafted 7zip file. **CVE ID : CVE-2019-1000019**	N/A	O-DEB-DEBI-020419/274
N/A	2019-02-04	4.3	libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c, read_CE()/parse_rockridge() that can result in DoS by infinite loop. This attack appears to be exploitable via the victim opening a specially crafted ISO9660 file. **CVE ID : CVE-2019-1000020**	N/A	O-DEB-DEBI-020419/275
N/A	2019-02-04	4.4	Debian tmpreaper version 1.6.13+nmu1 has a race condition when doing a (bind)	N/A	O-DEB-DEBI-020419/276

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mount via rename() which could result in local privilege escalation. Mounting via rename() could potentially lead to a file being placed elsewhereon the filesystem hierarchy (e.g. /etc/cron.d/) if the directory being cleaned up was on the same physical filesystem. Fixed versions include 1.6.13+nmu1+deb9u1 and 1.6.14. **CVE ID : CVE-2019-3461**		
N/A	2019-02-06	7.5	Insufficient sanitization of arguments passed to rsync can bypass the restrictions imposed by rssh, a restricted shell that should restrict users to perform only rsync operations, resulting in the execution of arbitrary shell commands. **CVE ID : CVE-2019-3463**	N/A	O-DEB-DEBI-020419/277
N/A	2019-02-06	7.5	Insufficient sanitization of environment variables passed to rsync can bypass the restrictions imposed by rssh, a restricted shell that should restrict users to perform only rsync operations, resulting in the execution of arbitrary shell commands. **CVE ID : CVE-2019-3464**	N/A	O-DEB-DEBI-020419/278
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in	N/A	O-DEB-DEBI-020419/279

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**		
N/A	2019-02-06	7.5	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header. **CVE ID : CVE-2019-3822**	N/A	O-DEB-DEBI-020419/280
N/A	2019-02-06	5	libcurl versions from 7.34.0 to	N/A	O-DEB-DEBI-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to \`smtp_endofresp()\` isn't NUL terminated and contains no character ending the parsed number, and \`len\` is set to 5, then the \`strtol()\` call reads beyond the allocated buffer. The read contents will not be returned to the caller. **CVE ID : CVE-2019-3823**		020419/281
N/A	2019-02-02	6.8	In Poppler 0.73.0, a heap-based buffer over-read (due to an integer signedness error in the XRef::getEntry function in XRef.cc) allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document, as demonstrated by pdftocairo. **CVE ID : CVE-2019-7310**	N/A	O-DEB-DEBI-020419/282
N/A	2019-02-03	7.5	liblivemedia in Live555 before 2019.02.03 mishandles the termination of an RTSP stream after RTP/RTCP-over-RTSP has been set up, which could lead to a Use-After-Free error that causes the RTSP server to crash (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2019-7314**	N/A	O-DEB-DEBI-020419/283

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in IMA_ADPCM_nibble in audio/SDL_wave.c. **CVE ID : CVE-2019-7572**	N/A	O-DEB-DEBI-020419/284
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (inside the wNumCoef loop). **CVE ID : CVE-2019-7573**	N/A	O-DEB-DEBI-020419/285
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in IMA_ADPCM_decode in audio/SDL_wave.c. **CVE ID : CVE-2019-7574**	N/A	O-DEB-DEBI-020419/286
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in MS_ADPCM_decode in audio/SDL_wave.c. **CVE ID : CVE-2019-7575**	N/A	O-DEB-DEBI-020419/287
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (outside the wNumCoef loop).	N/A	O-DEB-DEBI-020419/288

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7576		
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in SDL_LoadWAV_RW in audio/SDL_wave.c. **CVE ID : CVE-2019-7577**	N/A	O-DEB-DEBI-020419/289
N/A	2019-02-07	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitIMA_ADPCM in audio/SDL_wave.c. **CVE ID : CVE-2019-7578**	N/A	O-DEB-DEBI-020419/290
N/A	2019-02-08	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in Blit1to4 in video/SDL_blit_1.c. **CVE ID : CVE-2019-7635**	N/A	O-DEB-DEBI-020419/291
N/A	2019-02-08	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in SDL_GetRGB in video/SDL_pixels.c. **CVE ID : CVE-2019-7636**	N/A	O-DEB-DEBI-020419/292
N/A	2019-02-08	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in SDL_FillRect in video/SDL_surface.c. **CVE ID : CVE-2019-7637**	N/A	O-DEB-DEBI-020419/293
N/A	2019-02-08	6.8	SDL (Simple DirectMedia	N/A	O-DEB-DEBI-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in Map1toN in video/SDL_pixels.c. **CVE ID : CVE-2019-7638**		020419/294
N/A	2019-02-09	6.8	Genivia gSOAP 2.7.x and 2.8.x before 2.8.75 allows attackers to cause a denial of service (application abort) or possibly have unspecified other impact if a server application is built with the -DWITH_COOKIES flag. This affects the C/C++ libgsoapck/libgsoapck++ and libgsoapssl/libgsoapssl++ libraries, as these are built with that flag. **CVE ID : CVE-2019-7659**	https://www.genivia.com/advisory.html#Bug_in_gSOAP_versions_2.7.0_to_2.8.74_for_applications_built_with_the_WITH_COOKIES_flag_enabled_(Jan_14,_2019)	O-DEB-DEBI-020419/295
N/A	2019-02-09	4.3	An Invalid Address dereference was discovered in TIFFWriteDirectoryTagTransferfunction in libtiff/tif_dirwrite.c in LibTIFF 4.0.10, affecting the cpSeparateBufToContigBuf function in tiffcp.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. This is different from CVE-2018-12900. **CVE ID : CVE-2019-7663**	N/A	O-DEB-DEBI-020419/296
N/A	2019-02-09	4.3	In elfutils 0.175, a heap-based buffer over-read was discovered in the function	N/A	O-DEB-DEBI-020419/297

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elf32_xlatetom in elf32_xlatetom.c in libelf. A crafted ELF input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note does not reject malformed core file notes. **CVE ID : CVE-2019-7665**		
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**	N/A	O-DEB-DEBI-020419/298
Dlink					
dir-823g_firmware					
N/A	2019-02-01	9.3	An issue was discovered on D-Link DIR-823G devices with firmware through 1.02B03. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body, such as a body of ' /bin/telnetd' for the GetDeviceSettingsset API function. Consequently, an attacker can execute any command remotely when they control this input.	N/A	O-DLI-DIR--020419/299

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7298		
N/A	2019-02-04	5	An issue was discovered in /bin/goahead on D-Link DIR-823G devices with firmware 1.02B03. There is incorrect access control allowing remote attackers to get sensitive information (such as MAC address) about all clients in the WLAN via the GetClientInfo HNAP API. Consequently, an attacker can achieve information disclosure without authentication. **CVE ID : CVE-2019-7388**	N/A	O-DLI-DIR--020419/300
N/A	2019-02-04	7.8	An issue was discovered in /bin/goahead on D-Link DIR-823G devices with the firmware 1.02B03. There is incorrect access control allowing remote attackers to reset the router without authentication via the SetFactoryDefault HNAP API. Consequently, an attacker can achieve a denial-of-service attack without authentication. **CVE ID : CVE-2019-7389**	N/A	O-DLI-DIR--020419/301
N/A	2019-02-04	5	An issue was discovered in /bin/goahead on D-Link DIR-823G devices with firmware 1.02B03. There is incorrect access control allowing remote attackers to hijack the DNS service configuration of all clients in the WLAN, without authentication, via the	N/A	O-DLI-DIR--020419/302

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SetWanSettings HNAP API. **CVE ID : CVE-2019-7390**		
dir-600m_firmware					
N/A	2019-02-11	7.5	D-Link DIR-600M C1 3.04 devices allow authentication bypass via a direct request to the wan.htm page. **CVE ID : CVE-2019-7736**	N/A	O-DLI-DIR--020419/303
dir-878_firmware					
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the twsystem function with untrusted input from the request body for the SetSysLogSettings API function, as demonstrated by shell metacharacters in the IPAddress field. **CVE ID : CVE-2019-8312**	N/A	O-DLI-DIR--020419/304
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root	N/A	O-DLI-DIR--020419/305

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the twsystem function with untrusted input from the request body for the SetIPv6FirewallSettings API function, as demonstrated by shell metacharacters in the SrcIPv6AddressRangeStart field. **CVE ID : CVE-2019-8313**		
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetQoSSettings API function, as demonstrated by shell metacharacters in the IPAddress field. **CVE ID : CVE-2019-8314**	N/A	O-DLI-DIR--020419/306

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the twsystem function with untrusted input from the request body for the SetIPv4FirewallSettings API function, as demonstrated by shell metacharacters in the SrcIPv4AddressRangeStart field. **CVE ID : CVE-2019-8315**	N/A	O-DLI-DIR--020419/307
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the	N/A	O-DLI-DIR--020419/308

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SetWebFilterSettings API function, as demonstrated by shell metacharacters in the WebFilterURLs field. **CVE ID : CVE-2019-8316**		
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetStaticRouteIPv6Settings API function, as demonstrated by shell metacharacters in the DestNetwork field. **CVE ID : CVE-2019-8317**	N/A	O-DLI-DIR--020419/309
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This	N/A	O-DLI-DIR--020419/310

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			occurs when any HNAP API function triggers a call to the twsystem function with untrusted input from the request body for the SetSysEmailSettings API function, as demonstrated by shell metacharacters in the SMTPServerPort field. **CVE ID : CVE-2019-8318**		
N/A	2019-02-12	9	An issue was discovered on D-Link DIR-878 devices with firmware 1.12A1. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetStaticRouteIPv4Settings API function, as demonstrated by shell metacharacters in the Gateway field. **CVE ID : CVE-2019-8319**	N/A	O-DLI-DIR--020419/311
Fedoraproject					
Fedora					
N/A	2019-02-08	4.3	An issue was discovered in gsi-openssh-server 7.9p1 on Fedora 29. If PermitPAMUserChange is set	N/A	O-FED-FEDO-020419/312

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to yes in the /etc/gsissh/sshd_config file, logins succeed with a valid username and an incorrect password, even though a failure entry is recorded in the /var/log/messages file. **CVE ID : CVE-2019-7639**		
Lexmark					
6500e_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-6500-020419/313
cx310_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-CX31-020419/314
cx410_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-CX41-020419/315
cx510_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow	http://support.lexmark.com/ind	O-LEX-CX51-020419/316

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	ex?page=content&id=TE912	
mx31x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX31-020419/317
mx410_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX41-020419/318
mx510_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX51-020419/319
mx511_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX51-020419/320
mx610_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices	http://support.lexma	O-LEX-MX61-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	rk.com/index?page=content&id=TE912	020419/321
mx611_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX61-020419/322
mx6500e_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX65-020419/323
mx71x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX71-020419/324
mx81x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX81-020419/325
mx91x_firmware					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-MX91-020419/326
x46x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X46X-020419/327
x548_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X548-020419/328
x65x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X65X-020419/329
x73x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X73X-020419/330

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
x74x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X74X-020419/331
x792_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X792-020419/332
x86x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X86X-020419/333
x925_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-X925-020419/334
x95x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts.	http://support.lexmark.com/index?page=content&id=	O-LEX-X95X-020419/335

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6489	TE912	
xc2132_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XC21-020419/336
xm1145_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM11-020419/337
xm3150_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM31-020419/338
xm5163_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM51-020419/339
xm5170_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase	http://support.lexmark.com/index?page=c	O-LEX-XM51-020419/340

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stored shortcuts. **CVE ID : CVE-2019-6489**	ontent&id=TE912	
xm7155_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM71-020419/341
xm7155x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM71-020419/342
xm7163_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM71-020419/343
xm7163x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM71-020419/344
xm7170_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow	http://support.lexmark.com/ind	O-LEX-XM71-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	ex?page=content&id=TE912	020419/345
xm7170x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM71-020419/346
xm91x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XM91-020419/347
xs548_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XS54-020419/348
xs748_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XS74-020419/349
xs79x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices	http://support.lexma	O-LEX-XS79-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	rk.com/index?page=content&id=TE912	020419/350
xs925_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XS92-020419/351
xs95x_firmware					
N/A	2019-02-11	6.4	Certain Lexmark CX, MX, X, XC, XM, XS, and 6500e devices before 2019-02-11 allow remote attackers to erase stored shortcuts. **CVE ID : CVE-2019-6489**	http://support.lexmark.com/index?page=content&id=TE912	O-LEX-XS95-020419/352
Lifesize					
networker_220_firmware					
N/A	2019-02-08	9	LifeSize Team, Room, Passport, and Networker 220 devices allow Authenticated Remote OS Command Injection, as demonstrated by shell metacharacters in the support/mtusize.php mtu_size parameter. The lifesize default password for the cli account may sometimes be used for authentication. **CVE ID : CVE-2019-7632**	N/A	O-LIF-NETW-020419/353
passport_220_firmware					
N/A	2019-02-08	9	LifeSize Team, Room, Passport,	N/A	O-LIF-PASS-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Networker 220 devices allow Authenticated Remote OS Command Injection, as demonstrated by shell metacharacters in the support/mtusize.php mtu_size parameter. The lifesize default password for the cli account may sometimes be used for authentication. **CVE ID : CVE-2019-7632**		020419/354
room_220_firmware					
N/A	2019-02-08	9	LifeSize Team, Room, Passport, and Networker 220 devices allow Authenticated Remote OS Command Injection, as demonstrated by shell metacharacters in the support/mtusize.php mtu_size parameter. The lifesize default password for the cli account may sometimes be used for authentication. **CVE ID : CVE-2019-7632**	N/A	O-LIF-ROOM-020419/355
team_220_firmware					
N/A	2019-02-08	9	LifeSize Team, Room, Passport, and Networker 220 devices allow Authenticated Remote OS Command Injection, as demonstrated by shell metacharacters in the support/mtusize.php mtu_size parameter. The lifesize default password for the cli account may sometimes be used for authentication.	N/A	O-LIF-TEAM-020419/356

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7632		
Linux					
linux_kernel					
N/A	2019-02-15	6.8	In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because of a race condition, leading to a use-after-free. **CVE ID : CVE-2019-6974**	N/A	O-LIN-LINU-020419/357
N/A	2019-02-01	7.5	kernel/bpf/verifier.c in the Linux kernel before 4.20.6 performs undesirable out-of-bounds speculation on pointer arithmetic in various cases, including cases of different branches with different state or limits to sanitize, leading to side-channel attacks. **CVE ID : CVE-2019-7308**	N/A	O-LIN-LINU-020419/358
Mitsubishielectric					
q03udecpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack	N/A	O-MIT-Q03U-020419/359

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash. **CVE ID : CVE-2019-6535**		
q03udvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q03U-020419/360
q04udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q04U-020419/361
q04udpvcpu_firmware					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q04U-020419/362
q04udvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q04U-020419/363
q06udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU:	N/A	O-MIT-Q06U-020419/364

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**		
q06udpvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q06U-020419/365
q06udvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote	N/A	O-MIT-Q06U-020419/366

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**		
q100udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q100-020419/367
q10udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash.	N/A	O-MIT-Q10U-020419/368

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6535		
q13udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q13U-020419/369
q13udpvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q13U-020419/370
q13udvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU:	N/A	O-MIT-Q13U-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**		020419/371
q20udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q20U-020419/372
q26udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU,	N/A	O-MIT-Q26U-020419/373

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**		
q26udpvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q26U-020419/374
q26udvcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will	N/A	O-MIT-Q26U-020419/375

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**		
q50udehcpu_firmware					
N/A	2019-02-05	5	Mitsubishi Electric Q03/04/06/13/26UDVCPU: serial number 20081 and prior, Q04/06/13/26UDPVCPU: serial number 20081 and prior, and Q03UDECPU, Q04/06/10/13/20/26/50/100UDEHCPU: serial number 20101 and prior. A remote attacker can send specific bytes over Port 5007 that will result in an Ethernet stack crash. **CVE ID : CVE-2019-6535**	N/A	O-MIT-Q50U-020419/376
Mobotix					
s14_firmware					
N/A	2019-02-09	5	An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. Administrator Credentials are stored in the 13-character DES hash format. **CVE ID : CVE-2019-7673**	N/A	O-MOB-S14_-020419/377
N/A	2019-02-09	5	An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. /admin/access accepts a request to set the "aaaaa" password, considered insecure for some use cases, from a user. **CVE ID : CVE-2019-7674**	N/A	O-MOB-S14_-020419/378

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-09	5	An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. The default management application is delivered over cleartext HTTP with Basic Authentication, as demonstrated by the /admin/index.html URI. **CVE ID : CVE-2019-7675**	N/A	O-MOB-S14_-020419/379
Nttdocomo					
v20_pro_l-01j_firmware					
N/A	2019-02-13	5.7	V20 PRO L-01J software version L01J20c and L01J20d has a NULL pointer exception flaw that can be used by an attacker to cause the device to crash on the same network range via a specially crafted access point. **CVE ID : CVE-2019-5914**	N/A	O-NTT-V20_-020419/380
Redhat					
enterprise_linux_desktop					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	O-RED-ENTE-020419/381
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script	N/A	O-RED-ENTE-020419/382

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**		
enterprise_linux_server					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	O-RED-ENTE-020419/383
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe. **CVE ID : CVE-2019-5736**	N/A	O-RED-ENTE-020419/384
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x	N/A	O-RED-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**		ENTE-020419/385
enterprise_linux_server_aus					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	O-RED-ENTE-020419/386
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**	N/A	O-RED-ENTE-020419/387
enterprise_linux_server_eus					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	O-RED-ENTE-020419/388

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**	N/A	O-RED-ENTE-020419/389
enterprise_linux_server_tus					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	O-RED-ENTE-020419/390
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**	N/A	O-RED-ENTE-020419/391
enterprise_linux_workstation					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers.	N/A	O-RED-ENTE-020419/392

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3813		
N/A	2019-02-12	4.4	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file. **CVE ID : CVE-2019-8308**	N/A	O-RED-ENTE-020419/393
virtualization					
N/A	2019-02-04	5.4	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers. **CVE ID : CVE-2019-3813**	N/A	O-RED-VIRT-020419/394
enterprise_linux					
N/A	2019-02-06	6.9	A vulnerability was discovered in gdm before 3.31.4. When timed login is enabled in configuration, an attacker could bypass the lock screen by selecting the timed login user and waiting for the timer to expire, at which time they would gain access to the logged-in user's session. **CVE ID : CVE-2019-3825**	N/A	O-RED-ENTE-020419/395
N/A	2019-02-11	9.3	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently	N/A	O-RED-ENTE-020419/396

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe. **CVE ID : CVE-2019-5736**		
riot-os					
riot-os					
N/A	2019-02-04	7.5	RIOT RIOT-OS version after commit 7af03ab624db0412c727eed9ab7630a5282e2fd3 contains a Buffer Overflow vulnerability in sock_dns, an implementation of the DNS protocol utilizing the RIOT sock API that can result in Remote code executing. This attack appears to be exploitable via network connectivity. **CVE ID : CVE-2019-1000006**	N/A	O-RIO-RIOT-020419/397
systrome					
isg-600c_firmware					
N/A	2019-02-04	4	A local file inclusion vulnerability exists in the web interface of Systrome Cumilon	N/A	O-SYS-ISG--020419/398

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ISG-600C, ISG-600H, and ISG-800W 1.1-R2.1_TRUNK-20180914.bin devices. When the export function is called from system/maintenance/export.php, it accepts the path provided by the user, leading to path traversal via the name parameter. **CVE ID : CVE-2019-7387**		
isg-600h_firmware					
N/A	2019-02-04	4	A local file inclusion vulnerability exists in the web interface of Systrome Cumilon ISG-600C, ISG-600H, and ISG-800W 1.1-R2.1_TRUNK-20180914.bin devices. When the export function is called from system/maintenance/export.php, it accepts the path provided by the user, leading to path traversal via the name parameter. **CVE ID : CVE-2019-7387**	N/A	O-SYS-ISG--020419/399
isg-800w_firmware					
N/A	2019-02-04	4	A local file inclusion vulnerability exists in the web interface of Systrome Cumilon ISG-600C, ISG-600H, and ISG-800W 1.1-R2.1_TRUNK-20180914.bin devices. When the export function is called from system/maintenance/export.php, it accepts the path	N/A	O-SYS-ISG--020419/400

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provided by the user, leading to path traversal via the name parameter. **CVE ID : CVE-2019-7387**		
Hardware					
Cisco					
aironet_active_sensor					
N/A	2019-02-07	7.8	A vulnerability in the default configuration of the Cisco Aironet Active Sensor could allow an unauthenticated, remote attacker to restart the sensor. The vulnerability is due to a default local account with a static password. The account has privileges only to reboot the device. An attacker could exploit this vulnerability by guessing the account name and password to access the CLI. A successful exploit could allow the attacker to reboot the device repeatedly, creating a denial of service (DoS) condition. It is not possible to change the configuration or view sensitive data with this account. Versions prior to DNAC1.2.8 are affected. **CVE ID : CVE-2019-1675**	N/A	H-CIS-AIRO-020419/401