National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Aug 2019 Vol. 06 No. 15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
10web					
photo_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-08-2019	3.5	The 10Web Photo Gallery plugin before 1.5.23 for WordPress has authenticated stored XSS. **CVE ID : CVE-2019-14797**	N/A	A-10W-PHOT-220819/1
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-08-2019	4	The 10Web Photo Gallery plugin before 1.5.25 for WordPress has Authenticated Local File Inclusion via directory traversal in the wp-admin/admin-ajax.php?action=shortcode_bwg tagtext parameter. **CVE ID : CVE-2019-14798**	N/A	A-10W-PHOT-220819/2
3proxy					
3proxy					
Out-of-bounds Write	01-08-2019	7.5	webadmin.c in 3proxy before 0.8.13 has an out-of-bounds write in the admin interface. **CVE ID : CVE-2019-14495**	N/A	A-3PR-3PRO-220819/3
adenion					
blog2social					
Improper Neutralization of Special Elements	01-08-2019	7.5	The Adenion Blog2Social plugin through 5.5.0 for WordPress allows SQL	N/A	A-ADE-BLOG-220819/4

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Injection. **CVE ID : CVE-2019-13572**		
adplug_project					
adplug					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	6.8	AdPlug 2.3.1 has a heap-based buffer overflow in CxadbmfPlayer::__bmf_convert_stream() in bmf.cpp. **CVE ID : CVE-2019-14690**	N/A	A-ADP-ADPL-220819/5
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	6.8	AdPlug 2.3.1 has a heap-based buffer overflow in CdtmLoader::load() in dtm.cpp. **CVE ID : CVE-2019-14691**	N/A	A-ADP-ADPL-220819/6
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	6.8	AdPlug 2.3.1 has a heap-based buffer overflow in CmkjPlayer::load() in mkj.cpp. **CVE ID : CVE-2019-14692**	N/A	A-ADP-ADPL-220819/7
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	6.8	AdPlug 2.3.1 has multiple heap-based buffer overflows in Ca2mLoader::load() in a2m.cpp. **CVE ID : CVE-2019-14732**	N/A	A-ADP-ADPL-220819/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	6.8	AdPlug 2.3.1 has multiple heap-based buffer overflows in CradLoader::load() in rad.cpp. **CVE ID : CVE-2019-14733**	N/A	A-ADP-ADPL-220819/9
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	6.8	AdPlug 2.3.1 has multiple heap-based buffer overflows in CmtkLoader::load() in mtk.cpp. **CVE ID : CVE-2019-14734**	N/A	A-ADP-ADPL-220819/10
Advantech					
webaccess_hmi_designer					
Out-of-bounds Write	02-08-2019	6.8	In Advantech WebAccess HMI Designer Version 2.1.9.23 and prior, processing specially crafted MCR files lacking proper validation of user supplied data may cause the system to write outside the intended buffer area, allowing remote code execution. **CVE ID : CVE-2019-10961**	N/A	A-ADV-WEBA-220819/11
Apache					
tika					
Improper Restriction of Operations within the Bounds of a Memory	02-08-2019	6.8	A carefully crafted or corrupt zip file can cause an OOM in Apache Tika's RecursiveParserWrapper in versions 1.7-1.21. Users should upgrade to 1.22 or later.	N/A	A-APA-TIKA-220819/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			**CVE ID : CVE-2019-10088**		
Uncontrolled Resource Consumption	02-08-2019	4.3	In Apache Tika 1.19 to 1.21, a carefully crafted 2003ml or 2006ml file could consume all available SAXParsers in the pool and lead to very long hangs. Apache Tika users should upgrade to 1.22 or later. **CVE ID : CVE-2019-10093**	N/A	A-APA-TIKA-220819/13
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-08-2019	6.8	A carefully crafted package/compressed file that, when unzipped/uncompressed yields the same file (a quine), causes a StackOverflowError in Apache Tika's RecursiveParserWrapper in versions 1.7-1.21. Apache Tika users should upgrade to 1.22 or later. **CVE ID : CVE-2019-10094**	https://lists.apache.org/thread.html/fe876a649d9d36525dd097fe87ff4dcb3b82bb0fbb3a3d71fb72ef61@%3Cdev.tika.apache.org%3E	A-APA-TIKA-220819/14
spark					
N/A	07-08-2019	4.3	Prior to Spark 2.3.3, in certain situations Spark would write user data to local disk unencrypted, even if spark.io.encryption.enabled=true. This includes cached blocks that are fetched to disk (controlled by spark.maxRemoteBlockSizeFetchToMem); in SparkR, using parallelize; in Pyspark, using broadcast and parallelize; and use of python	N/A	A-APA-SPAR-220819/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			udfs. **CVE ID : CVE-2019-10099**		
solr					
Improper Authentication	01-08-2019	9	In Apache Solr, the DataImportHandler, an optional but popular module to pull in data from databases and other sources, has a feature in which the whole DIH configuration can come from a request's "dataConfig" parameter. The debug mode of the DIH admin screen uses this to allow convenient debugging / development of a DIH config. Since a DIH config can contain scripts, this parameter is a security risk. Starting with version 8.2.0 of Solr, use of this parameter requires setting the Java System property "enable.dih.dataConfigParam " to true. **CVE ID : CVE-2019-0193**	https://issues.apache.org/jira/browse/SOLR-13669	A-APA-SOLR-220819/16
ranger					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-08-2019	4.3	Policy import functionality in Apache Ranger 0.7.0 to 1.2.0 is vulnerable to a cross-site scripting issue. Upgrade to 2.0.0 or later version of Apache Ranger with the fix. **CVE ID : CVE-2019-12397**	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANG-220819/17
beardev					
joomsport					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-08-2019	7.5	The BearDev JoomSport plugin 3.3 for WordPress allows SQL injection to steal, modify, or delete database information via the joomsport_season/new-yorkers/?action=playerlist sid parameter. **CVE ID : CVE-2019-14348**	N/A	A-BEA-JOOM-220819/18
brandy_project					
brandy					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-08-2019	4.3	Brandy 1.20.1 has a stack-based buffer overflow in fileio_openout in fileio.c via crafted BASIC source code. **CVE ID : CVE-2019-14662**	N/A	A-BRA-BRAN-220819/19
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-08-2019	4.3	Brandy 1.20.1 has a stack-based buffer overflow in fileio_openin in fileio.c via crafted BASIC source code. **CVE ID : CVE-2019-14663**	N/A	A-BRA-BRAN-220819/20
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-08-2019	4.3	Brandy 1.20.1 has a heap-based buffer overflow in define_array in variables.c via crafted BASIC source code. **CVE ID : CVE-2019-14665**	N/A	A-BRA-BRAN-220819/21
Cisco					
webex_meetings_online					
Improper	07-08-2019	9.3	Multiple vulnerabilities in	N/A	A-CIS-WEBE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2019-1924**		220819/22
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-08-2019	9.3	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An	N/A	A-CIS-WEBE-220819/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2019-1925**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-08-2019	9.3	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the	N/A	A-CIS-WEBE-220819/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			targeted user. **CVE ID : CVE-2019-1926**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-08-2019	9.3	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2019-1927**	N/A	A-CIS-WEBE-220819/25
webex_meetings_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-08-2019	9.3	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist	N/A	A-CIS-WEBE-220819/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2019-1924**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-08-2019	9.3	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful	N/A	A-CIS-WEBE-220819/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2019-1925**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-08-2019	9.3	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2019-1926**	N/A	A-CIS-WEBE-220819/28
Improper Restriction of Operations within the Bounds of a	07-08-2019	9.3	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an	N/A	A-CIS-WEBE-220819/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			attacker to execute arbitrary code on an affected system. The vulnerabilities exist because the affected software improperly validates Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. An attacker could exploit these vulnerabilities by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user. **CVE ID : CVE-2019-1927**		
Codecabin					
wp_google_maps					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-08-2019	3.5	The WP Google Maps plugin before 7.11.35 for WordPress allows XSS via the wp-admin/ rectangle_name or rectangle_opacity parameter. **CVE ID : CVE-2019-14792**	N/A	A-COD-WP_G-220819/30
Codection					
import_users_from_csv_with_meta					
Cross-Site Request Forgery (CSRF)	08-08-2019	4.9	The codection "Import users from CSV with meta" plugin before 1.14.2.2 for WordPress allows wp-admin/admin-	N/A	A-COD-IMPO-220819/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ajax.php?action=acui_delete_attachment CSRF. **CVE ID : CVE-2019-14683**		
Codepeople					
appointment_booking_calendar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-08-2019	4.3	The Appointment Booking Calendar plugin 1.3.18 for WordPress allows XSS via the wp-admin/admin-post.php editionarea parameter. **CVE ID : CVE-2019-14791**	N/A	A-COD-APPO-220819/32
denx					
u-boot					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	6.8	In Das U-Boot versions 2016.11-rc1 through 2019.07-rc4, an underflow can cause memcpy() to overwrite a very large amount of data (including the whole stack) while reading a crafted ext4 filesystem. **CVE ID : CVE-2019-13104**	N/A	A-DEN-U-BO-220819/33
Double Free	06-08-2019	6.8	Das U-Boot versions 2019.07-rc1 through 2019.07-rc4 can double-free a cached block of data when listing files in a crafted ext4 filesystem. **CVE ID : CVE-2019-13105**	N/A	A-DEN-U-BO-220819/34
Out-of-bounds Write	06-08-2019	8.3	Das U-Boot versions 2016.09 through 2019.07-rc4 can memset() too much data while reading a crafted ext4 filesystem, which results in a stack buffer overflow and	N/A	A-DEN-U-BO-220819/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			likely code execution. **CVE ID : CVE-2019-13106**		
diaowen					
dwsurvey					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-08-2019	4.3	DWSurvey through 2019-07-22 has stored XSS via the design/my-survey-design!copySurvey.action surveyName parameter. **CVE ID : CVE-2019-14747**	N/A	A-DIA-DWSU-220819/36
Djangoproject					
django					
Improper Input Validation	02-08-2019	5	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If django.utils.text.Truncator's chars() and words() methods were passed the html=True argument, they were extremely slow to evaluate certain inputs due to a catastrophic backtracking vulnerability in a regular expression. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which were thus vulnerable. **CVE ID : CVE-2019-14232**	https://www.djangoproject.com/weblog/2019/aug/01/security-releases/	A-DJA-DJAN-220819/37
Improper Input Validation	02-08-2019	5	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. Due to the	https://www.djangoproject.com/webl	A-DJA-DJAN-220819/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			behaviour of the underlying HTMLParser, django.utils.html.strip_tags would be extremely slow to evaluate certain inputs containing large sequences of nested incomplete HTML entities. **CVE ID : CVE-2019-14233**	og/2019/aug/01/security-releases/	
Improper Input Validation	02-08-2019	5	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If passed certain inputs, django.utils.encoding.uri_to_iri could lead to significant memory usage due to a recursion when repercent-encoding invalid UTF-8 octet sequences. **CVE ID : CVE-2019-14235**	https://www.djangoproject.com/weblog/2019/aug/01/security-releases/	A-DJA-DJAN-220819/39
editor.md_project					
editor.md					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-08-2019	4.3	pandao Editor.md 1.5.0 allows XSS via the Javascript: string. **CVE ID : CVE-2019-14517**	N/A	A-EDI-EDIT-220819/40
emca					
energy_logserver					
Improper Limitation of a Pathname to a Restricted	05-08-2019	5	The api/admin/logoupload Logo File upload feature in EMCA Energy Logserver 6.1.2 allows attackers to send any kind of file to any location on	N/A	A-EMC-ENER-220819/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			the server via path traversal in the filename parameter. **CVE ID : CVE-2019-14521**		
Enigmail					
enigmail					
Inadequate Encryption Strength	05-08-2019	4.3	In Enigmail below 2.1, an attacker in possession of PGP encrypted emails can wrap them as sub-parts within a crafted multipart email. The encrypted part(s) can further be hidden using HTML/CSS or ASCII newline characters. This modified multipart email can be re-sent by the attacker to the intended receiver. If the receiver replies to this (benign looking) email, he unknowingly leaks the plaintext of the encrypted message part(s) back to the attacker. This attack variant bypasses protection mechanisms implemented after the "EFAIL" attacks. **CVE ID : CVE-2019-14664**	N/A	A-ENI-ENIG-220819/42
Espocrm					
espocrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	3.5	An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed when a attacker sends an attachment to admin with malicious JavaScript in the filename. This JavaScript executed when an admin selects the particular file from the list of all attachments. The attacker	N/A	A-ESP-ESPO-220819/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could inject the JavaScript inside the filename and send it to users, thus helping him steal victims' cookies (hence compromising their accounts). **CVE ID : CVE-2019-14547**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	3.5	An issue was discovered in EspoCRM before 5.6.9. Stored XSS in the body of an Article was executed when a victim opens articles received through mail. This Article can be formed by an attacker using the Knowledge Base feature in the tab list. The attacker could inject malicious JavaScript inside the body of the article, thus helping him steal victims' cookies (hence compromising their accounts). **CVE ID : CVE-2019-14548**	N/A	A-ESP-ESPO-220819/44
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	3.5	An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed inside the title and breadcrumb of a newly formed entity available to all the users. A malicious user can inject JavaScript in these values of an entity, thus stealing user cookies when someone visits the publicly accessible link. **CVE ID : CVE-2019-14549**	N/A	A-ESP-ESPO-220819/45
Improper Neutralization of Input	05-08-2019	3.5	An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed when a	N/A	A-ESP-ESPO-220819/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			victim clicks on the Edit Dashboard feature present on the Homepage. An attacker can load malicious JavaScript inside the add tab list feature, which would fire when a user clicks on the Edit Dashboard button, thus helping him steal victims' cookies (hence compromising their accounts). **CVE ID : CVE-2019-14550**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	3.5	An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed on the Preference page as well as while sending an email when a malicious payload was inserted inside the Email Signature in the Preference page. The attacker could insert malicious JavaScript inside his email signature, which fires when the victim replies or forwards the mail, thus helping him steal victims' cookies (hence compromising their accounts). **CVE ID : CVE-2019-14546**	N/A	A-ESP-ESPO-220819/47
Fedoraproject					
389_directory_server					
Uncontrolled Resource Consumption	02-08-2019	7.8	It was found that the fix for CVE-2018-14648 in 389-ds-base, versions 1.4.0.x before 1.4.0.17, was incorrectly applied in RHEL 7.5. An attacker would still be able to	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-	A-FED-389_-220819/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provoke excessive CPU consumption leading to a denial of service. **CVE ID : CVE-2019-10171**	10171	
firefly-iii					
flrefly_iii					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	4.3	Firefly III 4.7.17.4 is vulnerable to multiple stored XSS issues due to the lack of filtration of user-supplied data in the transaction description field and the asset account name. The JavaScript code is executed during a convert transaction action. **CVE ID : CVE-2019-14667**	N/A	A-FIR-FLRE-220819/49
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	3.5	Firefly III 4.7.17.3 is vulnerable to stored XSS due to the lack of filtration of user-supplied data in the transaction description field. The JavaScript code is executed during deletion of a transaction link. **CVE ID : CVE-2019-14668**	N/A	A-FIR-FLRE-220819/50
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	3.5	Firefly III 4.7.17.3 is vulnerable to stored XSS due to the lack of filtration of user-supplied data in the asset account name. The JavaScript code is executed during a visit to the audit account statistics page. **CVE ID : CVE-2019-14669**	N/A	A-FIR-FLRE-220819/51
Improper Neutralization of Input	05-08-2019	3.5	Firefly III 4.7.17.3 is vulnerable to stored XSS due to the lack of filtration of	N/A	A-FIR-FLRE-220819/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			user-supplied data in the bill name field. The JavaScript code is executed during rule-from-bill creation. **CVE ID : CVE-2019-14670**		
Information Exposure	05-08-2019	2.1	Firefly III 4.7.17.3 is vulnerable to local file enumeration. An attacker can enumerate local files due to the lack of protocol scheme sanitization, such as for file:/// URLs. This is related to fints_url to import/job/configuration, and import/create/fints. **CVE ID : CVE-2019-14671**	N/A	A-FIR-FLRE-220819/53
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	3.5	Firefly III 4.7.17.5 is vulnerable to stored XSS due to the lack of filtration of user-supplied data in the liability name field. The JavaScript code is executed upon an error condition during a visit to the account show page. **CVE ID : CVE-2019-14672**	N/A	A-FIR-FLRE-220819/54
Foliovision					
fv_flowplayer_video_player					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-08-2019	4.3	The FV Flowplayer Video Player plugin before 7.3.14.727 for WordPress allows email subscription XSS. **CVE ID : CVE-2019-14799**	N/A	A-FOL-FV_F-220819/55
Improper Neutralizatio	09-08-2019	7.5	The FV Flowplayer Video Player plugin before	N/A	A-FOL-FV_F-220819/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			7.3.15.727 for WordPress allows email subscription SQL injection. **CVE ID : CVE-2019-14801**		
Freedesktop					
poppler					
Divide By Zero	01-08-2019	4.3	An issue was discovered in Poppler through 0.78.0. There is a divide-by-zero error in the function SplashOutputDev::tilingPatternFill at SplashOutputDev.cc. **CVE ID : CVE-2019-14494**	N/A	A-FRE-POPP-220819/57
getwooplugins					
woo-variation-swatches					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-08-2019	4.3	The woo-variation-swatches (aka Variation Swatches for WooCommerce) plugin 1.0.61 for WordPress allows XSS via the wp-admin/admin.php?page=woo-variation-swatches-settings tab parameter. **CVE ID : CVE-2019-14774**	N/A	A-GET-WOO--220819/58
Gnome					
evolution-ews					
Improper Certificate Validation	01-08-2019	5.8	It was discovered evolution-ews before 3.31.3 does not check the validity of SSL certificates. An attacker could abuse this flaw to get confidential information by tricking the user into connecting to a fake server without the user noticing the	https://gitlab.gnome.org/GNOME/evolution-ews/issues/27	A-GNO-EVOL-220819/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			difference. **CVE ID : CVE-2019-3890**		
gnucobol_project					
gnucobol					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-08-2019	6.8	GnuCOBOL 2.2 has a buffer overflow in cb_push_op in cobc/field.c via crafted COBOL source code. **CVE ID : CVE-2019-14468**	N/A	A-GNU-GNUC-220819/60
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-08-2019	6.8	GnuCOBOL 2.2 has a buffer overflow in cb_evaluate_expr in cobc/field.c via crafted COBOL source code. **CVE ID : CVE-2019-14486**	N/A	A-GNU-GNUC-220819/61
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-08-2019	6.8	GnuCOBOL 2.2 has a heap-based buffer overflow in read_literal in cobc/scanner.l via crafted COBOL source code. **CVE ID : CVE-2019-14528**	N/A	A-GNU-GNUC-220819/62
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-08-2019	6.8	GnuCOBOL 2.2 has a stack-based buffer overflow in cb_encode_program_id in cobc/typeck.c via crafted COBOL source code. **CVE ID : CVE-2019-14541**	N/A	A-GNU-GNUC-220819/63
go-camo_project					
go-camo					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	08-08-2019	7.5	A Server Side Request Forgery (SSRF) vulnerability in go-camo up to version 1.1.4 allows a remote attacker to perform HTTP requests to internal endpoints. **CVE ID : CVE-2019-14255**	https://github.com/cactus/go-camo/security/advisories/GHSA-xrmp-4542-q746	A-GO--GO-C-220819/64
gogs					
gogs					
N/A	02-08-2019	7.5	routes/api/v1/api.go in Gogs 0.11.86 lacks permission checks for routes: deploy keys, collaborators, and hooks. **CVE ID : CVE-2019-14544**	N/A	A-GOG-GOGS-220819/65
Google					
cloud_messaging_notification					
N/A	07-08-2019	4	Jenkins Google Cloud Messaging Notification Plugin 1.0 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10379**	N/A	A-GOO-CLOU-220819/66
happypointcard					
happypoint					
Improper Control of Generation of Code ('Code	01-08-2019	5.8	When processing Deeplink scheme, Happypoint mobile app 6.3.19 and earlier versions doesn't check Deeplink URL correctly. This could lead to javascript code	https://www.boho.or.kr/krcert/secNoticeView.do?bulleti	A-HAP-HAPP-220819/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			execution, url redirection, sensitive information disclosure. An attacker can exploit this issue by enticing an unsuspecting user to open a specific malicious URL. **CVE ID : CVE-2019-9140**	n_writing_sequence=35103	
IBM					
jazz_for_service_management					
Improper Authorization	02-08-2019	2.1	IBM Jazz for Service Management 1.1.3, 1.1.3.1, and 1.1.3.2 could allow an unauthorized local user to create unique catalog names that could cause a denial of service. IBM X-Force ID: 160296. **CVE ID : CVE-2019-4275**	N/A	A-IBM-JAZZ-220819/68
java					
N/A	05-08-2019	4.6	Multiple binaries in IBM SDK, Java Technology Edition 7, 7R, and 8 on the AIX platform use insecure absolute RPATHs, which may facilitate code injection and privilege elevation by local users. IBM X-Force ID: 163984. **CVE ID : CVE-2019-4473**	N/A	A-IBM-JAVA-220819/69
websphere_mq					
Improper Input Validation	05-08-2019	4	IBM WebSphere MQ V7.1, 7.5, IBM MQ V8, IBM MQ V9.0LTS, IBM MQ V9.1 LTS, and IBM MQ V9.1 CD are vulnerable to a denial of service attack caused by specially crafted messages. IBM X-Force ID: 160013.	https://www.ibm.com/support/docview.wss?uid=ibm10886887	A-IBM-WEBS-220819/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4261		
cloud_private					
Information Exposure Through Log Files	05-08-2019	2.1	IBM Cloud Private 2.1.0 , 3.1.0, 3.1.1, and 3.1.2 could allow a local privileged user to obtain sensitive OIDC token that is printed to log files, which could be used to log in to the system as another user. IBM X-Force ID: 160512. **CVE ID : CVE-2019-4284**	https://www.ibm.com/support/docview.wss?uid=ibm10885454	A-IBM-CLOU-220819/71
imgtech					
zoneplayer					
Improper Input Validation	02-08-2019	7.5	ZInsVX.dll ActiveX Control 2018.02 and earlier in Zoneplayer contains a vulnerability that could allow remote attackers to execute arbitrary files by setting the arguments to the ActiveX method. This can be leveraged for remote code execution. **CVE ID : CVE-2019-9141**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35104	A-IMG-ZONE-220819/72
ipandao					
editor.md					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-08-2019	4.3	pandao Editor.md 1.5.0 allows XSS via an attribute of an ABBR or SUP element. **CVE ID : CVE-2019-14653**	N/A	A-IPA-EDIT-220819/73
Jenkins					
vmware_lab_manager_slaves					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	07-08-2019	5.8	Jenkins VMware Lab Manager Slaves Plugin 0.2.8 and earlier disables SSL/TLS and hostname verification globally for the Jenkins master JVM. **CVE ID : CVE-2019-10382**	N/A	A-JEN-VMWA-220819/74
relution_enterprise_appstore_publisher					
Cross-Site Request Forgery (CSRF)	07-08-2019	4.3	A cross-site request forgery vulnerability in Jenkins Relution Enterprise Appstore Publisher Plugin 1.24 and earlier allows attackers to have Jenkins initiate an HTTP connection to an attacker-specified server. **CVE ID : CVE-2019-10388**	N/A	A-JEN-RELU-220819/75
N/A	07-08-2019	4	A missing permission check in Jenkins Relution Enterprise Appstore Publisher Plugin 1.24 and earlier allows attackers to have Jenkins initiate an HTTP connection to an attacker-specified server. **CVE ID : CVE-2019-10389**	N/A	A-JEN-RELU-220819/76
configuration_as_code					
Information Exposure Through Log Files	07-08-2019	2.1	Due to an incomplete fix of CVE-2019-10343, Jenkins Configuration as Code Plugin 1.26 and earlier did not properly apply masking to some values expected to be hidden when logging the configuration being applied. **CVE ID : CVE-2019-10367**	N/A	A-JEN-CONF-220819/77
jclouds					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	07-08-2019	6.8	A cross-site request forgery vulnerability in Jenkins JClouds Plugin 2.14 and earlier in BlobStoreProfile.DescriptorImpl#doTestConnection and JCloudsCloud.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10368**	N/A	A-JEN-JCLO-220819/78
N/A	07-08-2019	4	A missing permission check in Jenkins JClouds Plugin 2.14 and earlier in BlobStoreProfile.DescriptorImpl#doTestConnection and JCloudsCloud.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10369**	N/A	A-JEN-JCLO-220819/79
mask_passwords					
N/A	07-08-2019	4.3	Jenkins Mask Passwords Plugin 2.12.0 and earlier transmits globally configured passwords in plain text as part of the configuration form, potentially resulting in their exposure.	N/A	A-JEN-MASK-220819/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10370		
gitlab_oauth					
Session Fixation	07-08-2019	5	A session fixation vulnerability in Jenkins Gitlab Authentication Plugin 1.4 and earlier in GitLabSecurityRealm.java allows unauthorized attackers to impersonate another user if they can control the pre-authentication session. **CVE ID : CVE-2019-10371**	N/A	A-JEN-GITL-220819/81
URL Redirection to Untrusted Site ('Open Redirect')	07-08-2019	5.8	An open redirect vulnerability in Jenkins Gitlab Authentication Plugin 1.4 and earlier in GitLabSecurityRealm.java allows attackers to redirect users to a URL outside Jenkins after successful login. **CVE ID : CVE-2019-10372**	N/A	A-JEN-GITL-220819/82
build_pipeline					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-08-2019	3.5	A stored cross-site scripting vulnerability in Jenkins Build Pipeline Plugin 1.5.8 and earlier allows attackers able to edit the build pipeline description to inject arbitrary HTML and JavaScript in the plugin-provided web pages in Jenkins. **CVE ID : CVE-2019-10373**	N/A	A-JEN-BUIL-220819/83
pegdown_formatter					
Improper Neutralization of Input During Web	07-08-2019	3.5	A stored cross-site scripting vulnerability in Jenkins PegDown Formatter Plugin 1.3 and earlier allows	N/A	A-JEN-PEGD-220819/84

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			attackers able to edit descriptions and other fields rendered using the configured markup formatter to insert links with the javascript scheme into the Jenkins UI. **CVE ID : CVE-2019-10374**		
file_system_scm					
Information Exposure	07-08-2019	4	An arbitrary file read vulnerability in Jenkins File System SCM Plugin 2.1 and earlier allows attackers able to configure jobs in Jenkins to obtain the contents of any file on the Jenkins master. **CVE ID : CVE-2019-10375**	N/A	A-JEN-FILE-220819/85
wall_display					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-08-2019	4.3	A reflected cross-site scripting vulnerability in Jenkins Wall Display Plugin 0.6.34 and earlier allows attackers to inject arbitrary HTML and JavaScript into web pages provided by this plugin. **CVE ID : CVE-2019-10376**	N/A	A-JEN-WALL-220819/86
avatar					
N/A	07-08-2019	4	A missing permission check in Jenkins Avatar Plugin 1.2 and earlier allows attackers with Overall/Read access to change the avatar of any user of Jenkins. **CVE ID : CVE-2019-10377**	N/A	A-JEN-AVAT-220819/87
testlink					
N/A	07-08-2019	2.1	Jenkins TestLink Plugin 3.16	N/A	A-JEN-TEST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10378**		220819/88
simple_travis_pipeline_runner					
N/A	07-08-2019	6.5	Jenkins Simple Travis Pipeline Runner Plugin 1.0 and earlier specifies unsafe values in its custom Script Security whitelist, allowing attackers able to execute Script Security protected scripts to execute arbitrary code. **CVE ID : CVE-2019-10380**	N/A	A-JEN-SIMP-220819/89
codefresh_integration					
Improper Certificate Validation	07-08-2019	4.3	Jenkins Codefresh Integration Plugin 1.8 and earlier disables SSL/TLS and hostname verification globally for the Jenkins master JVM. **CVE ID : CVE-2019-10381**	N/A	A-JEN-CODE-220819/90
eggplant					
N/A	07-08-2019	4	Jenkins eggPlant Plugin 2.2 and earlier stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10385**	N/A	A-JEN-EGGP-220819/91

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xl_testview					
Cross-Site Request Forgery (CSRF)	07-08-2019	6.8	A cross-site request forgery vulnerability in Jenkins XL TestView Plugin 1.2.0 and earlier in XLTestView.XLTestDescriptor#doTestConnection allows users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10386**	N/A	A-JEN-XL_T-220819/92
N/A	07-08-2019	4	A missing permission check in Jenkins XL TestView Plugin 1.2.0 and earlier in XLTestView.XLTestDescriptor#doTestConnection allows users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10387**	N/A	A-JEN-XL_T-220819/93
Joomla					
Joomla!					
Improper Input Validation	04-08-2019	6.5	In Joomla! 3.9.7 and 3.9.8, inadequate filtering allows users authorised to create custom fields to manipulate the filtering options and inject an unvalidated option. In other words, the filter attribute in subform fields allows remote code	N/A	A-JOO-JOOM-220819/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. This is fixed in 3.9.9. **CVE ID : CVE-2019-14654**		
kuaifan					
kuaifancms					
Improper Control of Generation of Code ('Code Injection')	07-08-2019	7.5	A issue was discovered in KuaiFanCMS 5.0. It allows eval injection by placing PHP code in the install.php db_name parameter and then making a config.php request. **CVE ID : CVE-2019-14746**	N/A	A-KUA-KUAI-220819/95
laquisscada					
scada					
Incorrect Type Conversion or Cast	05-08-2019	6.8	A type confusion vulnerability may be exploited when LAquis SCADA 4.3.1.71 processes a specially crafted project file. This may allow an attacker to execute remote code. The attacker must have local access to the system. A CVSS v3 base score of 7.8 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-10980**	N/A	A-LAQ-SCAD-220819/96
Out-of-bounds Read	05-08-2019	4.3	Processing a specially crafted project file in LAquis SCADA 4.3.1.71 may trigger an out-of-bounds read, which may allow an attacker to obtain sensitive information. The attacker must have local access to the system. A CVSS v3 base score of 2.5 has been	N/A	A-LAQ-SCAD-220819/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			calculated; the CVSS vector string is (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-10994**		
Magento					
magento					
Improper Input Validation	02-08-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to layouts can execute arbitrary code through a combination of product import, crafted csv file and XML layout update. **CVE ID : CVE-2019-7896**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/98
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to customer configurations to inject malicious javascript. **CVE ID : CVE-2019-7897**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/99
Improper Input Validation	02-08-2019	5	Samples of disabled downloadable products are accessible in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to	https://magento.com/security/patches/magento-2.3.2-	A-MAG-MAGE-220819/100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 due to inadequate validation of user input. **CVE ID : CVE-2019-7898**	2.2.9-and-2.1.18-security-update-23	
Improper Input Validation	02-08-2019	5	Names of disabled downloadable products could be disclosed due to inadequate validation of user input in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. **CVE ID : CVE-2019-7899**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/101
Improper Control of Generation of Code ('Code Injection')	02-08-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to email templates can execute arbitrary code by previewing a malicious template. **CVE ID : CVE-2019-7903**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/102
Improper Access Control	02-08-2019	5.5	Insufficient enforcement of user access controls in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could enable a low-privileged user to make unauthorized environment configuration changes. **CVE ID : CVE-2019-7904**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify product information. **CVE ID : CVE-2019-7908**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/104
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to email templates. **CVE ID : CVE-2019-7909**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/105
Server-Side Request Forgery (SSRF)	02-08-2019	6.5	A server-side request forgery (SSRF) vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to the admin panel to manipulate system configuration and execute arbitrary code. **CVE ID : CVE-2019-7911**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	02-08-2019	6.5	A file upload filter bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with admin privileges to edit configuration keys to remove file extension filters, potentially resulting in the malicious upload and execution of malicious files on the server. **CVE ID : CVE-2019-7912**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/107
Server-Side Request Forgery (SSRF)	02-08-2019	6.5	A server-side request forgery (SSRF) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with admin privileges to manipulate shipment methods to execute arbitrary code. **CVE ID : CVE-2019-7913**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/108
Improper Input Validation	02-08-2019	5	A denial-of-service vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. Under certain conditions, an unauthenticated attacker could force the Magento store's full page cache to serve a 404 page to customers. **CVE ID : CVE-2019-7915**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/109
Improper	02-08-2019	3.5	A stored cross-site scripting	https://m	A-MAG-MAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			vulnerability exists in the product catalog form of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to the product catalog to inject malicious javascript. **CVE ID : CVE-2019-7921**	agento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	220819/110
Server-Side Request Forgery (SSRF)	02-08-2019	6.5	A server-side request forgery (SSRF) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by authenticated user with admin privileges to manipulate shipment settings to execute arbitrary code. **CVE ID : CVE-2019-7923**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/111
N/A	02-08-2019	5.5	An insecure direct object reference (IDOR) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an administrator with limited privileges to delete the downloadable products folder. **CVE ID : CVE-2019-7925**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/112
Improper Neutralization of Input During Web Page	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3	https://magento.com/security/patches/magento	A-MAG-MAGE-220819/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify node attributes to inject malicious javascript. **CVE ID : CVE-2019-7926**	-2.3.2-2.2.9-and-2.1.18-security-update-23	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to edit product content pages to inject malicious javascript. **CVE ID : CVE-2019-7927**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/114
Improper Input Validation	02-08-2019	5	A denial-of-service (DoS) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. By abusing insufficient brute-forcing defenses in the token exchange protocol, an unauthenticated attacker could disrupt transactions between the Magento merchant and PayPal. **CVE ID : CVE-2019-7928**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/115
Information Exposure	02-08-2019	4	An information leakage vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges may be able to view metadata of a trusted device used by	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-	A-MAG-MAGE-220819/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another administrator via a crafted http request. **CVE ID : CVE-2019-7929**	update-33	
Unrestricted Upload of File with Dangerous Type	02-08-2019	9	A file upload restriction bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to the import feature can make modifications to a configuration file, resulting in potentially unauthorized removal of file upload restrictions. This can result in arbitrary code execution when a malicious file is then uploaded and executed on the system. **CVE ID : CVE-2019-7930**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/117
Improper Control of Generation of Code ('Code Injection')	02-08-2019	6.5	A remote code execution vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to create sitemaps can execute arbitrary PHP code by creating a malicious sitemap file. **CVE ID : CVE-2019-7932**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/118
Improper Neutralization of Input	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento	https://magento.com/securit	A-MAG-MAGE-220819/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to edit newsletter templates to inject malicious javascript. **CVE ID : CVE-2019-7934**	y/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify content page titles to inject malicious javascript. **CVE ID : CVE-2019-7935**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify content block titles to inject malicious javascript. **CVE ID : CVE-2019-7936**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/121
Improper Neutralization of Input	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1	https://magento.com/securit	A-MAG-MAGE-220819/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to store product attributes to inject malicious javascript. **CVE ID : CVE-2019-7937**	y/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify catalog price rules to inject malicious javascript. **CVE ID : CVE-2019-7938**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	4.3	A reflected cross-site scripting vulnerability exists on the customer cart checkout page of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by sending a victim a crafted URL that results in malicious javascript execution in the victim's browser. **CVE ID : CVE-2019-7939**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/124
Improper Neutralization of Input During Web	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2,	https://magento.com/security/patches	A-MAG-MAGE-220819/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify store currency options to inject malicious javascript. **CVE ID : CVE-2019-7940**	/magento-2.3.2-2.2.9-and-2.1.18-security-update-24	
Improper Control of Generation of Code ('Code Injection')	02-08-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to create or edit a product can execute arbitrary code via malicious XML layout updates. **CVE ID : CVE-2019-7942**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/126
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the product comments field of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to the Return Product comments field can inject malicious javascript. **CVE ID : CVE-2019-7944**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-24	A-MAG-MAGE-220819/127
Improper Neutralization of Input	02-08-2019	3.5	A stored cross-cite scripting vulnerability exists in Magento Open Source prior	https://magento.com/securit	A-MAG-MAGE-220819/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to modify currency symbols can inject malicious javascript. **CVE ID : CVE-2019-7945**	y/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	
Cross-Site Request Forgery (CSRF)	02-08-2019	4.3	A cross-site request forgery vulnerability exists in the GiftCardAccount removal feature for Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. **CVE ID : CVE-2019-7947**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/129
Improper Access Control	02-08-2019	5	An access control bypass vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An unauthenticated user can bypass access controls via REST API calls to assign themselves to an arbitrary company, thereby gaining read access to potentially confidental information. **CVE ID : CVE-2019-7950**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/130
Information Exposure	02-08-2019	5	An information leakage vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. A	https://magento.com/security/patches/magento	A-MAG-MAGE-220819/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SOAP web service endpoint does not properly enforce parameters related to access control. This could be abused to leak customer information via crafted SOAP requests. **CVE ID : CVE-2019-7951**	-2.3.2-2.2.9-and-2.1.18-security-update-13	
Session Fixation	02-08-2019	5	A defense-in-depth check was added to mitigate inadequate session validation handling by 3rd party checkout modules. This impacts Magento 1.x prior to 1.9.4.2, Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9 and Magento 2.3 prior to 2.3.2. **CVE ID : CVE-2019-7849**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/132
Cross-Site Request Forgery (CSRF)	02-08-2019	5.8	A cross-site request forgery vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can lead to unintended data deletion from customer pages. **CVE ID : CVE-2019-7851**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/133
Information Exposure	02-08-2019	5	A path disclosure vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. Requests for a specific file path could result in a redirect to the URL of the Magento admin panel, disclosing its location to potentially	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-	A-MAG-MAGE-220819/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized parties. **CVE ID : CVE-2019-7852**	33	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to the tax notifications configuration in the Magento admin panel. **CVE ID : CVE-2019-7853**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-24	A-MAG-MAGE-220819/135
Information Exposure	02-08-2019	5	An insecure direct object reference (IDOR) vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can lead to unauthorized disclosure of company credit history details. **CVE ID : CVE-2019-7854**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/136
N/A	02-08-2019	5	A cryptograhic flaw in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could be abused by an unauthenticated user to discover an invariant used in gift card generation. **CVE ID : CVE-2019-7855**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/137
Cross-Site Request Forgery (CSRF)	02-08-2019	4.3	A cross-site request forgery vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3	https://magento.com/security/patches	A-MAG-MAGE-220819/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 2.3.2 can cause unwanted items to be added to a shopper's cart due to an insufficiently robust anti-CSRF token implementation. **CVE ID : CVE-2019-7857**	/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	
N/A	02-08-2019	5	A cryptographic flaw in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9 and Magento 2.3 prior to 2.3.2 resulted in storage of sensitive information with an algorithm that is insufficiently resistant to brute force attacks. **CVE ID : CVE-2019-7858**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/139
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-08-2019	5	A path traversal vulnerability in the WYSIWYG editor for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could result in unauthorized access to uploaded images due to insufficient access control. **CVE ID : CVE-2019-7859**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-24	A-MAG-MAGE-220819/140
N/A	02-08-2019	5	A cryptographically weak pseudo-rando number generator is used in multiple security relevant contexts in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. **CVE ID : CVE-2019-7860**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	02-08-2019	5	Insufficient server-side validation of user input could allow an attacker to bypass file upload restrictions in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. **CVE ID : CVE-2019-7861**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/142
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A reflected cross-site scripting vulnerability exists in the Product widget chooser functionality in the admin panel for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. **CVE ID : CVE-2019-7862**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/143
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to products and categories. **CVE ID : CVE-2019-7863**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/144
Improper Access Control	02-08-2019	5	An insecure direct object reference (IDOR) vulnerability exists in the RSS feeds of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can lead to	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-	A-MAG-MAGE-220819/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to order details. **CVE ID : CVE-2019-7864**	2.1.18-security-update-33	
Cross-Site Request Forgery (CSRF)	02-08-2019	6.8	A cross-site request forgery (CSRF) vulnerability exists in the checkout cart item of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited at the time of editing or configuration. **CVE ID : CVE-2019-7865**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/146
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to edit Product information via the TinyMCE editor. **CVE ID : CVE-2019-7866**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/147
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to manage orders and order status. **CVE ID : CVE-2019-7867**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/148
Improper Neutralization of Input	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1	https://magento.com/securit	A-MAG-MAGE-220819/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with permissions to manage tax rules. **CVE ID : CVE-2019-7868**	y/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with permissions to manage customer groups. **CVE ID : CVE-2019-7869**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/150
N/A	02-08-2019	6.5	A security bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 that could be abused to execute arbitrary PHP code. An authenticated user can bypass security protections that prevent arbitrary PHP script upload via form data injection. **CVE ID : CVE-2019-7871**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/151
Improper Authorization	02-08-2019	5.5	An insecure direct object reference (IDOR) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 due to insufficient authorizations checks. This can be abused by a user with	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-	A-MAG-MAGE-220819/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			admin privileges to add users to company accounts or modify existing user details. **CVE ID : CVE-2019-7872**	update-13	
Cross-Site Request Forgery (CSRF)	02-08-2019	5.8	A cross-site request forgery vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can result in unintended deletion of the store design schedule. **CVE ID : CVE-2019-7873**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/153
Cross-Site Request Forgery (CSRF)	02-08-2019	4.3	A cross-site request forgery vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can result in unintended deletion of user roles. **CVE ID : CVE-2019-7874**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/154
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to newsletter templates. **CVE ID : CVE-2019-7875**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-08-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to manipulate layouts can insert a malicious payload into the layout. **CVE ID : CVE-2019-7876**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/156
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	4.3	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to manage orders can inject malicious javascript. **CVE ID : CVE-2019-7877**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/157
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to marketing email templates to inject malicious javascript. **CVE ID : CVE-2019-7880**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/158
Improper Neutralization of Input During Web Page Generation ('Cross-site	02-08-2019	3.5	A cross-site scripting mitigation bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user to	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-	A-MAG-MAGE-220819/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			escalate privileges (admin vs. admin XSS attack). **CVE ID : CVE-2019-7881**	2.1.18-security-update-23	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A stored cross-site scripting vulnerability exists in the WYSIWYG editor of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to the editor can inject malicious SWF files. **CVE ID : CVE-2019-7882**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/160
Improper Input Validation	02-08-2019	6.5	Insufficient input validation in the config builder of the Elastic search module could lead to remote code execution in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This vulnerability could be abused by an authenticated user with the ability to configure the catalog search. **CVE ID : CVE-2019-7885**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/161
N/A	02-08-2019	5	A cryptograhic flaw exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. A weak cryptograhic mechanism is used to generate the intialization vector in multiple security relevant contexts.	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-	A-MAG-MAGE-220819/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7886	33	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	3.5	A reflected cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 when the feature that adds a secret key to the Admin URL is disabled. **CVE ID : CVE-2019-7887**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/163
Information Exposure	02-08-2019	4	An information disclosure vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to create email templates could leak sensitive data via a malicious email template. **CVE ID : CVE-2019-7888**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-33	A-MAG-MAGE-220819/164
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-08-2019	4	An injection vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with marketing manipulation privileges can invoke methods that alter data of the underlying model followed by corresponding database modifications.	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7889		
N/A	02-08-2019	7.5	An Insecure Direct Object Reference (IDOR) vulnerability exists in the order processing workflow of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can lead to unauthorized access to order details. **CVE ID : CVE-2019-7890**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-23	A-MAG-MAGE-220819/166
Server-Side Request Forgery (SSRF)	02-08-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to access shipment settings can execute arbitrary code via server-side request forgery. **CVE ID : CVE-2019-7892**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/167
Improper Input Validation	02-08-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to layouts can execute arbitrary code through a crafted XML layout update. **CVE ID : CVE-2019-7895**	https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13	A-MAG-MAGE-220819/168
metabox					
meta_box					
Improper Access	09-08-2019	5.5	The Meta Box plugin before 4.16.3 for WordPress allows file deletion via ajax, with the	N/A	A-MET-META-220819/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			wp-admin/admin-ajax.php?action=rwmb_delete_file attachment_id parameter. **CVE ID : CVE-2019-14793**		
N/A	09-08-2019	5	The Meta Box plugin before 4.16.2 for WordPress mishandles the uploading of files to custom folders. **CVE ID : CVE-2019-14794**	N/A	A-MET-META-220819/170
Microfocus					
content_manager					
Improper Access Control	07-08-2019	5.5	Remote Access Control Bypass in Micro Focus Content Manager. versions 9.1, 9.2, 9.3. The vulnerability could be exploited to manipulate data stored during another user?s CheckIn request. **CVE ID : CVE-2019-11653**	https://softwaresupport.softwaregrp.com/doc/KM03489552	A-MIC-CONT-220819/171
mijnpress					
admin-renamer-extended					
Cross-Site Request Forgery (CSRF)	08-08-2019	3.5	The admin-renamer-extended (aka Admin renamer extended) plugin 3.2.1 for WordPress allows wp-admin/plugins.php?page=admin-renamer-extended/admin.php CSRF. **CVE ID : CVE-2019-14680**	N/A	A-MIJ-ADMI-220819/172
milkytracker_project					
milkytracker					
Improper Restriction of	01-08-2019	6.8	LoaderXM::load in LoaderXM.cpp in milkyplay in MilkyTracker 1.02.00 has a	N/A	A-MIL-MILK-220819/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			stack-based buffer overflow. **CVE ID : CVE-2019-14496**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-08-2019	6.8	ModuleEditor::convertInstrument in tracker/ModuleEditor.cpp in MilkyTracker 1.02.00 has a heap-based buffer overflow. **CVE ID : CVE-2019-14497**	N/A	A-MIL-MILK-220819/174
Mongodb					
mongodb					
Improper Authorization	06-08-2019	6	After user deletion in MongoDB Server the improper invalidation of authorization sessions allows an authenticated user's session to persist and become conflated with new accounts, if those accounts reuse the names of deleted ones. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.9; v3.6 versions prior to 3.6.13; v3.4 versions prior to 3.4.22. **CVE ID : CVE-2019-2386**	N/A	A-MON-MONG-220819/175
mq-woocommerce-products-price-bulk-edit_project					
mq-woocommerce-products-price-bulk-edit					
Improper Neutralization of Input During Web Page Generation	09-08-2019	3.5	The mq-woocommerce-products-price-bulk-edit (aka Woocommerce Products Price Bulk Edit) plugin 2.0 for WordPress allows XSS via the wp-admin/admin-	N/A	A-MQ--MQ-W-220819/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			ajax.php?action=update_options show_products_page_limit parameter. **CVE ID : CVE-2019-14796**		
Netapp					
oncommand_insight					
Information Exposure	09-08-2019	4	OnCommand Insight versions through 7.3.6 may disclose sensitive account information to an authenticated user. **CVE ID : CVE-2019-5498**	https://security.netapp.com/advisory/ntap-20190809-0001/	A-NET-ONCO-220819/177
Nextcloud					
lookup-server					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-08-2019	7.5	An SQL Injection in the Nextcloud Lookup-Server < v0.3.0 (running on https://lookup.nextcloud.com) caused unauthenticated users to be able to execute arbitrary SQL commands. **CVE ID : CVE-2019-5476**	N/A	A-NEX-LOOK-220819/178
Nvidia					
gpu_driver					
N/A	06-08-2019	7.2	NVIDIA Windows GPU Display Driver (all versions) contains a vulnerability in the user mode video driver trace logger component. When an attacker has access to the system and creates a hard link, the software does not check for hard link attacks. This behavior may lead to code execution, denial	https://support.lenovo.com/us/en/product_security/LEN-28096	A-NVI-GPU_-220819/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service, or escalation of privileges. **CVE ID : CVE-2019-5683**		
Out-of-bounds Write	06-08-2019	10	NVIDIA Windows GPU Display Driver (all versions) contains a vulnerability in DirectX drivers, in which a specially crafted shader can cause an out of bounds access of an input texture array, which may lead to denial of service or code execution. **CVE ID : CVE-2019-5684**	N/A	A-NVI-GPU_-220819/180
Out-of-bounds Write	06-08-2019	10	NVIDIA Windows GPU Display Driver (all versions) contains a vulnerability in DirectX drivers, in which a specially crafted shader can cause an out of bounds access to a shader local temporary array, which may lead to denial of service or code execution. **CVE ID : CVE-2019-5685**	N/A	A-NVI-GPU_-220819/181
Improper Input Validation	06-08-2019	4.9	NVIDIA Windows GPU Display Driver (all versions) contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the software uses an API function or data structure in a way that relies on properties that are not always guaranteed to be valid, which may lead to denial of service. **CVE ID : CVE-2019-5686**	https://support.lenovo.com/us/en/product_security/LEN-28096	A-NVI-GPU_-220819/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	06-08-2019	3.6	NVIDIA Windows GPU Display Driver (all versions) contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which an incorrect use of default permissions for an object exposes it to an unintended actor **CVE ID : CVE-2019-5687**	https://support.lenovo.com/us/en/product_security/LEN-28096	A-NVI-GPU_-220819/183
octopus					
octopus_deploy					
Information Exposure	05-08-2019	4	In Octopus Deploy 2019.4.0 through 2019.6.x before 2019.6.6, and 2019.7.x before 2019.7.6, an authenticated system administrator is able to view sensitive values by visiting a server configuration page or making an API call. **CVE ID : CVE-2019-14525**	https://octopus.com/downloads/compare?from=2019.6.6&to=2019.7.7	A-OCT-OCTO-220819/184
Opencv					
opencv					
Out-of-bounds Read	01-08-2019	6.4	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read in the function cv::predictOrdered<cv::HaarEvaluator> in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service. **CVE ID : CVE-2019-14491**	N/A	A-OPE-OPEN-220819/185
Out-of-bounds	01-08-2019	6.4	An issue was discovered in OpenCV before 3.4.7 and 4.x	N/A	A-OPE-OPEN-220819/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			before 4.1.1. There is an out of bounds read/write in the function HaarEvaluator::OptFeature::calc in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service. **CVE ID : CVE-2019-14492**		
NULL Pointer Dereference	01-08-2019	5	An issue was discovered in OpenCV before 4.1.1. There is a NULL pointer dereference in the function cv::XMLParser::parse at modules/core/src/persistence.cpp. **CVE ID : CVE-2019-14493**	N/A	A-OPE-OPEN-220819/187
Open-emr					
openemr					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-08-2019	7.5	OpenEMR before 5.0.2 allows SQL Injection in interface/forms/eye_mag/save.php. **CVE ID : CVE-2019-14529**	N/A	A-OPE-OPEN-220819/188
Open-school					
open-school					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-08-2019	4.3	Open-School 3.0, and Community Edition 2.3, allows XSS via the osv/index.php?r=students/guardians/create id parameter. **CVE ID : CVE-2019-14696**	N/A	A-OPE-OPEN-220819/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-08-2019	7.5	Open-School 3.0, and Community Edition 2.3, allows SQL Injection via the index.php?r=students/students/document id parameter. **CVE ID : CVE-2019-14754**	N/A	A-OPE-OPEN-220819/190
Osticket					
osticket					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-08-2019	3.5	An issue was discovered in osTicket before 1.10.7 and 1.12.x before 1.12.1. The Ticket creation form allows users to upload files along with queries. It was found that the file-upload functionality has fewer (or no) mitigations implemented for file content checks; also, the output is not handled properly, causing persistent XSS that leads to cookie stealing or malicious actions. For example, a non-agent user can upload a .html file, and Content-Disposition will be set to inline instead of attachment. **CVE ID : CVE-2019-14748**	N/A	A-OST-OSTI-220819/191
Improper Neutralization of Special Elements in Output Used by a Downstream Component	07-08-2019	6.8	An issue was discovered in osTicket before 1.10.7 and 1.12.x before 1.12.1. CSV (aka Formula) injection exists in the export spreadsheets functionality. These spreadsheets are generated dynamically from unvalidated or unfiltered	N/A	A-OST-OSTI-220819/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			user input in the Name and Internal Notes fields in the Users tab, and the Issue Summary field in the tickets tab. This allows other agents to download data in a .csv file format or .xls file format. This is used as input for spreadsheet applications such as Excel and OpenOffice Calc, resulting in a situation where cells in the spreadsheets can contain input from an untrusted source. As a result, the end user who is accessing the exported spreadsheet can be affected. **CVE ID : CVE-2019-14749**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-08-2019	4.3	An issue was discovered in osTicket before 1.10.7 and 1.12.x before 1.12.1. Stored XSS exists in setup/install.php. It was observed that no input sanitization was provided in the firstname and lastname fields of the application. The insertion of malicious queries in those fields leads to the execution of those queries. This can further lead to cookie stealing or other malicious actions. **CVE ID : CVE-2019-14750**	N/A	A-OST-OSTI-220819/193
palletsprojects					
werkzeug					
Insufficient Entropy	09-08-2019	5	Pallets Werkzeug before 0.15.3, when used with	N/A	A-PAL-WERK-220819/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Docker, has insufficient debugger PIN randomness because Docker containers share the same machine id. **CVE ID : CVE-2019-14806**		
pivotal_software					
application_service					
N/A	05-08-2019	5	Cloud Foundry UAA versions prior to v73.4.0 contain a vulnerability where a malicious client possessing the ?clients.write? authority or scope can bypass the restrictions imposed on clients created via ?clients.write? and create clients with arbitrary scopes that he does not possess. **CVE ID : CVE-2019-11270**	https://www.cloudfoundry.org/blog/cve-2019-11270	A-PIV-APPL-220819/195
cloud_foundry_uaa					
N/A	05-08-2019	5	Cloud Foundry UAA versions prior to v73.4.0 contain a vulnerability where a malicious client possessing the ?clients.write? authority or scope can bypass the restrictions imposed on clients created via ?clients.write? and create clients with arbitrary scopes that he does not possess. **CVE ID : CVE-2019-11270**	https://www.cloudfoundry.org/blog/cve-2019-11270	A-PIV-CLOU-220819/196
operations_manager					
N/A	05-08-2019	5	Cloud Foundry UAA versions prior to v73.4.0 contain a vulnerability where a malicious client possessing the ?clients.write? authority	https://www.cloudfoundry.org/blog/cve-2019-	A-PIV-OPER-220819/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or scope can bypass the restrictions imposed on clients created via ?clients.write? and create clients with arbitrary scopes that he does not possess. **CVE ID : CVE-2019-11270**	11270	
Radare					
radare2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-08-2019	6.8	In radare2 before 3.7.0, a command injection vulnerability exists in bin_symbols() in libr/core/cbin.c. By using a crafted executable file, it's possible to execute arbitrary shell commands with the permissions of the victim. This vulnerability is due to improper handling of symbol names embedded in executables. **CVE ID : CVE-2019-14745**	N/A	A-RAD-RADA-220819/198
Redhat					
openshift_container_platform					
Cross-Site Request Forgery (CSRF)	02-08-2019	5.8	A flaw was found in OpenShift Container Platform, versions 3.11 and later, in which the CSRF tokens used in the cluster console component were found to remain static during a user's session. An attacker with the ability to observe the value of this token would be able to re-use the token to perform a CSRF attack. **CVE ID : CVE-2019-10176**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10176	A-RED-OPEN-220819/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libvirt					
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	A-RED-LIBV-220819/200
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	A-RED-LIBV-220819/201
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervis	https://bugzilla.redhat.com/show_bu	A-RED-LIBV-220819/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			orCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**	g.cgi?id=CVE-2019-10168	
openshift					
Improper Authentication	01-08-2019	5	A vulnerability exists in the garbage collection mechanism of atomic-openshift. An attacker able spoof the UUID of a valid object from another namespace is able to delete children of those objects. Versions 3.6, 3.7, 3.8, 3.9, 3.10, 3.11 and 4.1 are affected. **CVE ID : CVE-2019-3884**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3884	A-RED-OPEN-220819/203
schben					
adive					
Cross-Site Request Forgery (CSRF)	06-08-2019	4.3	Internal/Views/config.php in Schben Adive 2.0.7 allows admin/config CSRF to change a user password. **CVE ID : CVE-2019-14346**	N/A	A-SCH-ADIV-220819/204
N/A	06-08-2019	6.5	Internal/Views/addUsers.php in Schben Adive 2.0.7 allows remote unprivileged	N/A	A-SCH-ADIV-220819/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users (editor or developer) to create an administrator account via admin/user/add, as demonstrated by a Python PoC script. **CVE ID : CVE-2019-14347**		
schismtracker					
schism_tracker					
Integer Underflow (Wrap or Wraparound)	02-08-2019	6.8	An issue was discovered in Schism Tracker through 20190722. There is an integer underflow via a large plen in fmt_okt_load_song in the Amiga Oktalyzer parser in fmt/okt.c. **CVE ID : CVE-2019-14523**	N/A	A-SCH-SCHI-220819/206
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-08-2019	6.8	An issue was discovered in Schism Tracker through 20190722. There is a heap-based buffer overflow via a large number of song patterns in fmt_mtm_load_song in fmt/mtm.c, a different vulnerability than CVE-2019-14465. **CVE ID : CVE-2019-14524**	N/A	A-SCH-SCHI-220819/207
Siemens					
siprotec_5_digsi_device_driver					
Improper Access Control	02-08-2019	7.5	A vulnerability has been identified in Ethernet plug-in communication modules for SIPROTEC 5 devices with CPU variants CP200 (All versions), SIPROTEC 5 devices with CPU variants CP300 (All versions). An unauthenticated attacker	N/A	A-SIE-SIPR-220819/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access to the device could potentially insert arbitrary code which is executed before firmware verification in the device. **CVE ID : CVE-2019-10938**		
Sitecore					
cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-08-2019	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Sitecore CMS 9.0.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) #300583 - List Manager Dashboard module, (2) #307638 - Campaign Creator module, (3) #316994 - Attributes field, (4) I#316995 - Icon Selection module, (5) #317000 - Latitude field, (6) #317000 - Longitude field, (7) #317017 - UploadPackage2.aspx module, (8) #317072 - Context menu, or (9) I#317073 - Insert from Template dialog. **CVE ID : CVE-2019-11198**	N/A	A-SIT-CMS-220819/209
Sleuthkit					
the_sleuth_kit					
Out-of-bounds Read	02-08-2019	7.5	An issue was discovered in The Sleuth Kit (TSK) 4.6.6. There is an out of bounds read on iso9660 while parsing System Use Sharing Protocol data in fs/iso9660.c. **CVE ID : CVE-2019-14531**	N/A	A-SLE-THE_-220819/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	02-08-2019	7.5	An issue was discovered in The Sleuth Kit (TSK) 4.6.6. There is an off-by-one overwrite due to an underflow on tools/hashtools/hfind.cpp while using a bogus hash table. **CVE ID : CVE-2019-14532**	N/A	A-SLE-THE_-220819/211
sygnoos					
popup_builder					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-08-2019	7.5	A SQL injection vulnerability exists in the Sygnoos Popup Builder plugin before 3.45 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via com/libs/Table.php because Subscribers Table ordering is mishandled. **CVE ID : CVE-2019-14695**	N/A	A-SYG-POPU-220819/212
Teampass					
teampass					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-08-2019	3.5	An issue was discovered in TeamPass 2.1.27.35. From the sources/items.queries.php "Import items" feature, it is possible to load a crafted CSV file with an XSS payload. **CVE ID : CVE-2019-12950**	N/A	A-TEA-TEAM-220819/213
Testlink					
testlink					
Improper	01-08-2019	4.3	TestLink 1.9.19 has XSS via	N/A	A-TES-TEST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			the error.php message parameter. **CVE ID : CVE-2019-14471**		220819/214
Thekelleys					
dnsmasq					
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-08-2019	5	Improper bounds checking in Dnsmasq before 2.76 allows an attacker controlled DNS server to send large DNS packets that result in a read operation beyond the buffer allocated for the packet, a different vulnerability than CVE-2017-14491. **CVE ID : CVE-2019-14513**	N/A	A-THE-DNSM-220819/215
ultimatemember					
ultimate_member					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-08-2019	3.5	The ultimate-member plugin before 2.0.54 for WordPress has XSS. **CVE ID : CVE-2019-14945**	N/A	A-ULT-ULTI-220819/216
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-08-2019	3.5	The ultimate-member plugin before 2.0.52 for WordPress has XSS related to UM Roles create and edit operations. **CVE ID : CVE-2019-14946**	N/A	A-ULT-ULTI-220819/217
Improper	12-08-2019	3.5	The ultimate-member plugin	N/A	A-ULT-ULTI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			before 2.0.52 for WordPress has XSS during an account upgrade. **CVE ID : CVE-2019-14947**		220819/218
UNA					
una					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-08-2019	3.5	studio/polyglot.php?page=etemplates in UNA 10.0.0-RC1 allows XSS via the System Name field under Emails during template editing. **CVE ID : CVE-2019-14804**	N/A	A-UNA-UNA-220819/219
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-08-2019	3.5	studio/builder_menu.php?page=sets in UNA 10.0.0-RC1 allows XSS via the System Name field under Sets during set editing. **CVE ID : CVE-2019-14805**	N/A	A-UNA-UNA-220819/220
webcraftic					
woody_ad_snippets					
N/A	08-08-2019	6.4	admin/includes/class.actions.snippet.php in the "Woody ad snippets" plugin through 2.2.5 for WordPress allows wp-admin/admin-post.php?action=close&post=deletion. **CVE ID : CVE-2019-14773**	N/A	A-WEB-WOOD-220819/221
Webkul					
bagisto					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	11-08-2019	6.8	Bagisto 0.1.5 allows CSRF under /admin URIs. **CVE ID : CVE-2019-14933**	N/A	A-WEB-BAGI-220819/222
wpseeds					
wp_database_backup					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-08-2019	4.3	The wp-database-backup plugin before 5.1.2 for WordPress has XSS. **CVE ID : CVE-2019-14949**	N/A	A-WPS-WP_D-220819/223
Yourls					
Yourls					
Improper Authentication	07-08-2019	7.5	YOURLS through 1.7.3 is affected by a type juggling vulnerability in the api component that can result in login bypass. **CVE ID : CVE-2019-14537**	N/A	A-YOU-YOUR-220819/224
Zurmo					
zurmo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-08-2019	4.3	Zurmo 3.2.7-2 has XSS via the app/index.php/zurmo/default PATH_INFO. **CVE ID : CVE-2019-14472**	N/A	A-ZUR-ZURM-220819/225
Operating System					
al-enterprise					
8008_firmware					
Improper	01-08-2019	7.7	On the Alcatel-Lucent	N/A	O-AL--8008-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			Enterprise (ALE) 8008 Cloud Edition Deskphone VoIP phone with firmware 1.50.13, a command injection (missing input validation) issue in the password change field for the Change Password interface allows an authenticated remote attacker in the same network to trigger OS commands via shell commands in a POST request. **CVE ID : CVE-2019-14260**		220819/226
Dell					
inspiron_7580_firmware					
Improper Access Control	05-08-2019	7.2	Select Dell Client Commercial and Consumer platforms contain an Improper Access Vulnerability. An unauthenticated attacker with physical access to the system could potentially bypass intended Secure Boot restrictions to run unsigned and untrusted code on expansion cards installed in the system during platform boot. Refer to https://www.dell.com/support/article/us/en/04/sln317683/dsa-2019-043-dell-client-improper-access-control-vulnerability?lang=en for versions affected by this vulnerability. **CVE ID : CVE-2019-3717**	https://www.dell.com/support/article/us/en/04/sln317683/dsa-2019-043-dell-client-improper-access-control-vulnerability?lang=en	O-DEL-INSP-220819/227
latitude_7214_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	05-08-2019	7.2	Select Dell Client Commercial and Consumer platforms contain an Improper Access Vulnerability. An unauthenticated attacker with physical access to the system could potentially bypass intended Secure Boot restrictions to run unsigned and untrusted code on expansion cards installed in the system during platform boot. Refer to https://www.dell.com/support/article/us/en/04/sln317683/dsa-2019-043-dell-client-improper-access-control-vulnerability?lang=en for versions affected by this vulnerability. **CVE ID : CVE-2019-3717**	https://www.dell.com/support/article/us/en/04/sln317683/dsa-2019-043-dell-client-improper-access-control-vulnerability?lang=en	O-DEL-LATI-220819/228
Dlink					
6600-ap_firmware					
Inadequate Encryption Strength	01-08-2019	4.6	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is use of weak ciphers for SSH such as diffie-hellman-group1-sha1. **CVE ID : CVE-2019-14332**	N/A	O-DLI-6600-220819/229
Improper Input Validation	01-08-2019	4.9	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a pre-authenticated denial of service attack against the access point via a long action	N/A	O-DLI-6600-220819/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter to admin.cgi. **CVE ID : CVE-2019-14333**		
Improper Certificate Validation	01-08-2019	2.1	An issue was discovered on D-Link 6600-AP, DWL-3600AP, and DWL-8610AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated Certificate and RSA Private Key extraction through an insecure sslcert-get.cgi HTTP command. **CVE ID : CVE-2019-14334**	N/A	O-DLI-6600-220819/231
Improper Authenticati on	08-08-2019	4.9	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated denial of service leading to the reboot of the AP via the admin.cgi?action=%s URI. **CVE ID : CVE-2019-14335**	N/A	O-DLI-6600-220819/232
Improper Input Validation	01-08-2019	2.1	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated dump of all of the config files through a certain admin.cgi?action= insecure HTTP request. **CVE ID : CVE-2019-14336**	N/A	O-DLI-6600-220819/233
N/A	01-08-2019	2.1	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is an ability to escape to a shell in the restricted command line interface, as demonstrated by the	N/A	O-DLI-6600-220819/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`/bin/sh -c wget` sequence. **CVE ID : CVE-2019-14337**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-08-2019	4.3	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a post-authentication admin.cgi?action= XSS vulnerability on the management interface. **CVE ID : CVE-2019-14338**	N/A	O-DLI-6600-220819/235
dwl-3600ap_firmware					
Inadequate Encryption Strength	01-08-2019	4.6	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is use of weak ciphers for SSH such as diffie-hellman-group1-sha1. **CVE ID : CVE-2019-14332**	N/A	O-DLI-DWL--220819/236
Improper Input Validation	01-08-2019	4.9	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a pre-authenticated denial of service attack against the access point via a long action parameter to admin.cgi. **CVE ID : CVE-2019-14333**	N/A	O-DLI-DWL--220819/237
Improper Certificate Validation	01-08-2019	2.1	An issue was discovered on D-Link 6600-AP, DWL-3600AP, and DWL-8610AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated Certificate and RSA Private Key extraction through an insecure sslcert-get.cgi HTTP command.	N/A	O-DLI-DWL--220819/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-14334		
Improper Authenticati on	08-08-2019	4.9	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated denial of service leading to the reboot of the AP via the admin.cgi?action=%s URI. **CVE ID : CVE-2019-14335**	N/A	O-DLI-DWL--220819/239
Improper Input Validation	01-08-2019	2.1	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated dump of all of the config files through a certain admin.cgi?action= insecure HTTP request. **CVE ID : CVE-2019-14336**	N/A	O-DLI-DWL--220819/240
N/A	01-08-2019	2.1	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is an ability to escape to a shell in the restricted command line interface, as demonstrated by the `/bin/sh -c wget` sequence. **CVE ID : CVE-2019-14337**	N/A	O-DLI-DWL--220819/241
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-08-2019	4.3	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a post-authentication admin.cgi?action= XSS vulnerability on the management interface.	N/A	O-DLI-DWL--220819/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-14338		
dwl-8610ap_firmware					
Improper Certificate Validation	01-08-2019	2.1	An issue was discovered on D-Link 6600-AP, DWL-3600AP, and DWL-8610AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated Certificate and RSA Private Key extraction through an insecure sslcert-get.cgi HTTP command. **CVE ID : CVE-2019-14334**	N/A	O-DLI-DWL--220819/243
dva-5592_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-08-2019	4.3	The web interface of the D-Link DVA-5592 20180823 is vulnerable to XSS because HTML form parameters are directly reflected. **CVE ID : CVE-2019-6968**	N/A	O-DLI-DVA--220819/244
Information Exposure	02-08-2019	5	The web interface of the D-Link DVA-5592 20180823 is vulnerable to an authentication bypass that allows an unauthenticated user to have access to sensitive information such as the Wi-Fi password and the phone number (if VoIP is in use). **CVE ID : CVE-2019-6969**	N/A	O-DLI-DVA--220819/245
eq-3					
ccu2_firmware					
Improper Authorization	06-08-2019	6.5	eQ-3 Homematic CCU2 and CCU3 use session IDs for authentication but lack authorization checks.	N/A	O-EQ--CCU2-220819/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consequently, a valid guest level or user level account can create a new admin level account, read the service messages, clear the system protocol or modify/delete internal programs, etc. pp. **CVE ID : CVE-2019-14473**		
Improper Authorization	05-08-2019	5	eQ-3 Homematic CCU2 2.47.15 and prior and CCU3 3.47.15 and prior use session IDs for authentication but lack authorization checks. An attacker can obtain a session ID from CVE-2019-9583, resulting in the ability to read the service messages, clear the system protocol, create a new user in the system, or modify/delete internal programs. **CVE ID : CVE-2019-14475**	N/A	O-EQ--CCU2-220819/247
ccu3_firmware					
Improper Authorization	06-08-2019	6.5	eQ-3 Homematic CCU2 and CCU3 use session IDs for authentication but lack authorization checks. Consequently, a valid guest level or user level account can create a new admin level account, read the service messages, clear the system protocol or modify/delete internal programs, etc. pp. **CVE ID : CVE-2019-14473**	N/A	O-EQ--CCU3-220819/248
Improper Authorization	05-08-2019	5	eQ-3 Homematic CCU2 2.47.15 and prior and CCU3 3.47.15 and prior use session IDs for authentication but	N/A	O-EQ--CCU3-220819/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack authorization checks. An attacker can obtain a session ID from CVE-2019-9583, resulting in the ability to read the service messages, clear the system protocol, create a new user in the system, or modify/delete internal programs. **CVE ID : CVE-2019-14475**		
HP					
hp2910al-48g_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-08-2019	3.5	A potential security vulnerability has been identified in HP2910al-48G version W.15.14.0016. The attack exploits an xss injection by setting the attack vector in one of the switch persistent configuration fields (management URL, location, contact). But admin privileges are required to configure these fields thereby reducing the likelihood of exploit. HPE Aruba has provided firmware updates to resolve the vulnerability in HP 2910-48G al Switch. Please update to W.15.14.0017. **CVE ID : CVE-2019-5401**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03944en_us	O-HP-HP29-220819/250
microdigital					
mdc-n2190v_firmware					
Improper Restriction of Operations within the	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. In a CGI program running under the	N/A	O-MIC-MDC--220819/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			HTTPD web server, a buffer overflow in the param parameter leads to remote code execution in the context of the nobody account. **CVE ID : CVE-2019-14698**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-08-2019	10	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker can exploit OS Command Injection in the filename parameter for remote code execution as root. This occurs in the Mainproc executable file, which can be run from the HTTPD web server. **CVE ID : CVE-2019-14699**	N/A	O-MIC-MDC--220819/252
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-08-2019	5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. There is disclosure of the existence of arbitrary files via Path Traversal in HTTPD. This occurs because the filename specified in the TZ parameter is accessed with a substantial delay if that file exists. **CVE ID : CVE-2019-14700**	N/A	O-MIC-MDC--220819/253
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-08-2019	5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker can trigger read operations on an arbitrary file via Path Traversal in the TZ parameter, but cannot	N/A	O-MIC-MDC--220819/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			retrieve the data that is read. This causes a denial of service if the filename is, for example, /dev/random. **CVE ID : CVE-2019-14701**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. SQL injection vulnerabilities exist in 13 forms that are reachable through HTTPD. An attacker can, for example, create an admin account. **CVE ID : CVE-2019-14702**	N/A	O-MIC-MDC--220819/255
Cross-Site Request Forgery (CSRF)	06-08-2019	6.8	A CSRF issue was discovered in webparam?user&action=set&param=add in HTTPD on MicroDigital N-series cameras with firmware through 6400.0.8.5 to create an admin account. **CVE ID : CVE-2019-14703**	N/A	O-MIC-MDC--220819/256
Server-Side Request Forgery (SSRF)	06-08-2019	7.5	An SSRF issue was discovered in HTTPD on MicroDigital N-series cameras with firmware through 6400.0.8.5 via FTP commands following a newline character in the uploadfile field. **CVE ID : CVE-2019-14704**	N/A	O-MIC-MDC--220819/257
Improper Access Control	06-08-2019	6.5	An Incorrect Access Control issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5 because any valid cookie can be used	N/A	O-MIC-MDC--220819/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to make requests as an admin. **CVE ID : CVE-2019-14705**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	5	A denial of service issue in HTTPD was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker without authorization can upload a file to upload.php with a filename longer than 256 bytes. This will be placed in the updownload area. It will not be deleted, because of a buffer overflow in a Bash command string. **CVE ID : CVE-2019-14706**	N/A	O-MIC-MDC--220819/259
N/A	06-08-2019	6.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. The firmware update process is insecure, leading to remote code execution. The attacker can provide arbitrary firmware in a .dat file via a webparam?system&action=set&upgrade URI. **CVE ID : CVE-2019-14707**	N/A	O-MIC-MDC--220819/260
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. A buffer overflow in the action parameter leads to remote code execution in the context of the nobody account. **CVE ID : CVE-2019-14708**	N/A	O-MIC-MDC--220819/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	06-08-2019	5	A cleartext password storage issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. The file in question is /usr/local/ipsca/mipsca.db. If a camera is compromised, the attacker can gain access to passwords and abuse them to compromise further systems. **CVE ID : CVE-2019-14709**	N/A	O-MIC-MDC--220819/262
mdc-n4090_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. In a CGI program running under the HTTPD web server, a buffer overflow in the param parameter leads to remote code execution in the context of the nobody account. **CVE ID : CVE-2019-14698**	N/A	O-MIC-MDC--220819/263
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-08-2019	10	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker can exploit OS Command Injection in the filename parameter for remote code execution as root. This occurs in the Mainproc executable file, which can be run from the HTTPD web server. **CVE ID : CVE-2019-14699**	N/A	O-MIC-MDC--220819/264
Improper	06-08-2019	5	An issue was discovered on	N/A	O-MIC-MDC--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			MicroDigital N-series cameras with firmware through 6400.0.8.5. There is disclosure of the existence of arbitrary files via Path Traversal in HTTPD. This occurs because the filename specified in the TZ parameter is accessed with a substantial delay if that file exists. **CVE ID : CVE-2019-14700**		220819/265
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-08-2019	5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker can trigger read operations on an arbitrary file via Path Traversal in the TZ parameter, but cannot retrieve the data that is read. This causes a denial of service if the filename is, for example, /dev/random. **CVE ID : CVE-2019-14701**	N/A	O-MIC-MDC--220819/266
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. SQL injection vulnerabilities exist in 13 forms that are reachable through HTTPD. An attacker can, for example, create an admin account. **CVE ID : CVE-2019-14702**	N/A	O-MIC-MDC--220819/267
Cross-Site Request Forgery (CSRF)	06-08-2019	6.8	A CSRF issue was discovered in webparam?user&action=set&param=add in HTTPD on MicroDigital N-series	N/A	O-MIC-MDC--220819/268

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cameras with firmware through 6400.0.8.5 to create an admin account. **CVE ID : CVE-2019-14703**		
Server-Side Request Forgery (SSRF)	06-08-2019	7.5	An SSRF issue was discovered in HTTPD on MicroDigital N-series cameras with firmware through 6400.0.8.5 via FTP commands following a newline character in the uploadfile field. **CVE ID : CVE-2019-14704**	N/A	O-MIC-MDC--220819/269
Improper Access Control	06-08-2019	6.5	An Incorrect Access Control issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5 because any valid cookie can be used to make requests as an admin. **CVE ID : CVE-2019-14705**	N/A	O-MIC-MDC--220819/270
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	5	A denial of service issue in HTTPD was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker without authorization can upload a file to upload.php with a filename longer than 256 bytes. This will be placed in the updownload area. It will not be deleted, because of a buffer overflow in a Bash command string. **CVE ID : CVE-2019-14706**	N/A	O-MIC-MDC--220819/271
N/A	06-08-2019	6.5	An issue was discovered on MicroDigital N-series	N/A	O-MIC-MDC--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cameras with firmware through 6400.0.8.5. The firmware update process is insecure, leading to remote code execution. The attacker can provide arbitrary firmware in a .dat file via a webparam?system&action=set&upgrade URI. **CVE ID : CVE-2019-14707**		220819/272
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. A buffer overflow in the action parameter leads to remote code execution in the context of the nobody account. **CVE ID : CVE-2019-14708**	N/A	O-MIC-MDC--220819/273
N/A	06-08-2019	5	A cleartext password storage issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. The file in question is /usr/local/ipsca/mipsca.db. If a camera is compromised, the attacker can gain access to passwords and abuse them to compromise further systems. **CVE ID : CVE-2019-14709**	N/A	O-MIC-MDC--220819/274
mdc-n4090w_firmware					
Improper Restriction of Operations within the Bounds of a	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. In a CGI program running under the HTTPD web server, a buffer	N/A	O-MIC-MDC--220819/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			overflow in the param parameter leads to remote code execution in the context of the nobody account. **CVE ID : CVE-2019-14698**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-08-2019	10	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker can exploit OS Command Injection in the filename parameter for remote code execution as root. This occurs in the Mainproc executable file, which can be run from the HTTPD web server. **CVE ID : CVE-2019-14699**	N/A	O-MIC-MDC--220819/276
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-08-2019	5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. There is disclosure of the existence of arbitrary files via Path Traversal in HTTPD. This occurs because the filename specified in the TZ parameter is accessed with a substantial delay if that file exists. **CVE ID : CVE-2019-14700**	N/A	O-MIC-MDC--220819/277
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-08-2019	5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker can trigger read operations on an arbitrary file via Path Traversal in the TZ parameter, but cannot retrieve the data that is read.	N/A	O-MIC-MDC--220819/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This causes a denial of service if the filename is, for example, /dev/random. **CVE ID : CVE-2019-14701**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. SQL injection vulnerabilities exist in 13 forms that are reachable through HTTPD. An attacker can, for example, create an admin account. **CVE ID : CVE-2019-14702**	N/A	O-MIC-MDC--220819/279
Cross-Site Request Forgery (CSRF)	06-08-2019	6.8	A CSRF issue was discovered in webparam?user&action=set&param=add in HTTPD on MicroDigital N-series cameras with firmware through 6400.0.8.5 to create an admin account. **CVE ID : CVE-2019-14703**	N/A	O-MIC-MDC--220819/280
Server-Side Request Forgery (SSRF)	06-08-2019	7.5	An SSRF issue was discovered in HTTPD on MicroDigital N-series cameras with firmware through 6400.0.8.5 via FTP commands following a newline character in the uploadfile field. **CVE ID : CVE-2019-14704**	N/A	O-MIC-MDC--220819/281
Improper Access Control	06-08-2019	6.5	An Incorrect Access Control issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5 because any valid cookie can be used to make requests as an	N/A	O-MIC-MDC--220819/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			admin. **CVE ID : CVE-2019-14705**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	5	A denial of service issue in HTTPD was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. An attacker without authorization can upload a file to upload.php with a filename longer than 256 bytes. This will be placed in the updownload area. It will not be deleted, because of a buffer overflow in a Bash command string. **CVE ID : CVE-2019-14706**	N/A	O-MIC-MDC--220819/283
N/A	06-08-2019	6.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. The firmware update process is insecure, leading to remote code execution. The attacker can provide arbitrary firmware in a .dat file via a webparam?system&action=set&upgrade URI. **CVE ID : CVE-2019-14707**	N/A	O-MIC-MDC--220819/284
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-08-2019	7.5	An issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. A buffer overflow in the action parameter leads to remote code execution in the context of the nobody account. **CVE ID : CVE-2019-14708**	N/A	O-MIC-MDC--220819/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	06-08-2019	5	A cleartext password storage issue was discovered on MicroDigital N-series cameras with firmware through 6400.0.8.5. The file in question is /usr/local/ipsca/mipsca.db. If a camera is compromised, the attacker can gain access to passwords and abuse them to compromise further systems. **CVE ID : CVE-2019-14709**	N/A	O-MIC-MDC--220819/286
Netapp					
data_ontap					
Information Exposure	02-08-2019	4.3	Data ONTAP operating in 7-Mode versions prior to 8.2.5P3 are susceptible to a vulnerability which discloses information to an unauthenticated attacker. A successful attack requires that multiple non-default options be enabled. **CVE ID : CVE-2019-5493**	https://security.netapp.com/advisory/ntap-20190801-0002/	O-NET-DATA-220819/287
Information Exposure	02-08-2019	5	Data ONTAP operating in 7-Mode versions prior to 8.2.5P3 may disclose sensitive LDAP account information to unauthenticated remote attackers. **CVE ID : CVE-2019-5501**	https://security.netapp.com/advisory/ntap-20190801-0001/	O-NET-DATA-220819/288
N/A	05-08-2019	6.4	SMB in Data ONTAP operating in 7-Mode versions prior to 8.2.5P3 has weak cryptography which when exploited could lead to information disclosure or	N/A	O-NET-DATA-220819/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			addition or modification of data. **CVE ID : CVE-2019-5502**		
Opensuse					
leap					
Improper Input Validation	02-08-2019	5	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If django.utils.text.Truncator's chars() and words() methods were passed the html=True argument, they were extremely slow to evaluate certain inputs due to a catastrophic backtracking vulnerability in a regular expression. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which were thus vulnerable. **CVE ID : CVE-2019-14232**	https://www.djangoproject.com/weblog/2019/aug/01/security-releases/	O-OPE-LEAP-220819/290
Improper Input Validation	02-08-2019	5	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. Due to the behaviour of the underlying HTMLParser, django.utils.html.strip_tags would be extremely slow to evaluate certain inputs containing large sequences of nested incomplete HTML entities. **CVE ID : CVE-2019-14233**	https://www.djangoproject.com/weblog/2019/aug/01/security-releases/	O-OPE-LEAP-220819/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-08-2019	5	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If passed certain inputs, django.utils.encoding.uri_to_iri could lead to significant memory usage due to a recursion when repercent-encoding invalid UTF-8 octet sequences. **CVE ID : CVE-2019-14235**	https://www.djangoproject.com/weblog/2019/aug/01/security-releases/	O-OPE-LEAP-220819/292
Polycom					
obihai_obi1022_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-08-2019	7.7	On the Polycom Obihai Obi1022 VoIP phone with firmware 5.1.11, a command injection (missing input validation) issue in the NTP server IP address field for the "Time Service Settings web" interface allows an authenticated remote attacker in the same network to trigger OS commands via shell commands in a POST request. **CVE ID : CVE-2019-14259**	N/A	O-POL-OBIH-220819/293
Redhat					
enterprise_linux_desktop					
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	O-RED-ENTE-220819/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**		
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-ENTE-220819/295
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10168	O-RED-ENTE-220819/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**		
enterprise_linux_server					
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	O-RED-ENTE-220819/297
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-ENTE-220819/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			own privileges. **CVE ID : CVE-2019-10167**		
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10168	O-RED-ENTE-220819/299
enterprise_linux_server_aus					
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	O-RED-ENTE-220819/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-ENTE-220819/301
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10168	O-RED-ENTE-220819/302
enterprise_linux_server_eus					
Improper Access	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before	https://bugzilla.re	O-RED-ENTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**	dhat.com/show_bug.cgi?id=CVE-2019-10166	220819/303
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-ENTE-220819/304
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator"	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10168	O-RED-ENTE-220819/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**		
Uncontrolled Resource Consumption	02-08-2019	7.8	It was found that the fix for CVE-2018-14648 in 389-ds-base, versions 1.4.0.x before 1.4.0.17, was incorrectly applied in RHEL 7.5. An attacker would still be able to provoke excessive CPU consumption leading to a denial of service. **CVE ID : CVE-2019-10171**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10171	O-RED-ENTE-220819/306
enterprise_linux_server_tus					
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	O-RED-ENTE-220819/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10166		
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-ENTE-220819/308
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10168	O-RED-ENTE-220819/309
enterprise_linux_workstation					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	O-RED-ENTE-220819/310
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-ENTE-220819/311
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x	https://bugzilla.redhat.com/show_bug.cgi?id=C	O-RED-ENTE-220819/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**	VE-2019-10168	
virtualization					
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	O-RED-VIRT-220819/313
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-VIRT-220819/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**		
Improper Access Control	02-08-2019	4.6	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10168	O-RED-VIRT-220819/315
enterprise_linux					
Improper Certificate Validation	01-08-2019	5.8	It was discovered evolution-ews before 3.31.3 does not check the validity of SSL certificates. An attacker could abuse this flaw to get confidential information by tricking the user into connecting to a fake server without the user noticing the	https://gitlab.gnome.org/GNOME/evolution-ews/issues/27	O-RED-ENTE-220819/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			difference. **CVE ID : CVE-2019-3890**		
Improper Access Control	02-08-2019	4.6	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed. **CVE ID : CVE-2019-10166**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10166	O-RED-ENTE-220819/317
Improper Access Control	02-08-2019	4.6	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10167**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10167	O-RED-ENTE-220819/318
Improper Access	02-08-2019	4.6	The virConnectBaselineHyperviso	https://bugzilla.re	O-RED-ENTE-220819/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			rCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges. **CVE ID : CVE-2019-10168**	dhat.com/show_bug.cgi?id=CVE-2019-10168	
shenzhen_dragon_brothers					
fb50_firmware					
N/A	06-08-2019	9	An HTTP parameter pollution issue was discovered on Shenzhen Dragon Brothers Fingerprint Bluetooth Round Padlock FB50 2.3. With the user ID, user name, and the lock's MAC address, anyone can unbind the existing owner of the lock, and bind themselves instead. This leads to complete takeover of the lock. The user ID, name, and MAC address are trivially obtained from APIs found within the Android or iOS application. With only the MAC address of the lock, any attacker can transfer ownership of the lock from the current user, over to the attacker's account. Thus	N/A	O-SHE-FB50-220819/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rendering the lock completely inaccessible to the current user. **CVE ID : CVE-2019-13143**		
tcl					
alcatel_linkzone_firmware					
Improper Authenticati on	02-08-2019	7.5	The web interface of Alcatel LINKZONE MW40-V-V1.0 MW40_LU_02.00_02 devices is vulnerable to an authentication bypass that allows an unauthenticated user to have access to the web interface without knowing the administrator's password. **CVE ID : CVE-2019-7163**	N/A	O-TCL-ALCA-220819/321
Windriver					
vxworks					
Argument Injection or Modification	05-08-2019	4.8	Wind River VxWorks 6.6, 6.7, 6.8, 6.9.3, 6.9.4, and Vx7 has Incorrect Access Control in IPv4 assignment by the ipdhcpc DHCP client component. **CVE ID : CVE-2019-12264**	https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/	O-WIN-VXWO-220819/322