National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 31 Mar 2019 Vol. 06 No. 06

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
OS					
abus					
secvest_wireless_alarm_system_fuaa50000_firmware					
N/A	27-03-2019	3.3	An issue was discovered on ABUS Secvest wireless alarm system FUAA50000 3.01.01 in conjunction with Secvest remote control FUBE50014 or FUBE50015. Because "encrypted signal transmission" is missing, an attacker is able to eavesdrop sensitive data as cleartext (for instance, the current rolling code state). **CVE ID : CVE-2019-9862**	N/A	O-ABU-SECV-040419/1
N/A	27-03-2019	10	Due to the use of an insecure algorithm for rolling codes in the ABUS Secvest wireless alarm system FUAA50000 3.01.01 and its remote controls FUBE50014 and FUBE50015, an attacker is able to predict valid future rolling codes, and can thus remotely control the alarm system in an unauthorized way. **CVE ID : CVE-2019-9863**	N/A	O-ABU-SECV-040419/2

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
secvest_wireless_remote_control_fube50014_firmware					
N/A	27-03-2019	3.3	An issue was discovered on ABUS Secvest wireless alarm system FUAA50000 3.01.01 in conjunction with Secvest remote control FUBE50014 or FUBE50015. Because "encrypted signal transmission" is missing, an attacker is able to eavesdrop sensitive data as cleartext (for instance, the current rolling code state). **CVE ID : CVE-2019-9862**	N/A	O-ABU-SECV-040419/3
N/A	27-03-2019	10	Due to the use of an insecure algorithm for rolling codes in the ABUS Secvest wireless alarm system FUAA50000 3.01.01 and its remote controls FUBE50014 and FUBE50015, an attacker is able to predict valid future rolling codes, and can thus remotely control the alarm system in an unauthorized way. **CVE ID : CVE-2019-9863**	N/A	O-ABU-SECV-040419/4
secvest_wireless_remote_control_fube50015_firmware					
N/A	27-03-2019	3.3	An issue was discovered on ABUS Secvest wireless alarm system FUAA50000 3.01.01 in conjunction with Secvest remote control FUBE50014 or	N/A	O-ABU-SECV-040419/5

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FUBE50015. Because "encrypted signal transmission" is missing, an attacker is able to eavesdrop sensitive data as cleartext (for instance, the current rolling code state). **CVE ID : CVE-2019-9862**		
N/A	27-03-2019	10	Due to the use of an insecure algorithm for rolling codes in the ABUS Secvest wireless alarm system FUAA50000 3.01.01 and its remote controls FUBE50014 and FUBE50015, an attacker is able to predict valid future rolling codes, and can thus remotely control the alarm system in an unauthorized way. **CVE ID : CVE-2019-9863**	N/A	O-ABU-SECV-040419/6
audiocodes					
420hd_ip_phone_firmware					
N/A	21-03-2019	3.5	AudioCodes IP phone 420HD devices using firmware version 2.2.12.126 allow XSS. **CVE ID : CVE-2018-10091**	N/A	O-AUD-420H-040419/7
N/A	21-03-2019	9	AudioCodes IP phone 420HD devices using firmware version 2.2.12.126 allow Remote Code Execution.	N/A	O-AUD-420H-040419/8

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-10093		
Canonical					
ubuntu_linux					
N/A	27-03-2019	4.9	It was discovered that Dovecot before versions 2.2.36.1 and 2.3.4.1 incorrectly handled client certificates. A remote attacker in possession of a valid certificate with an empty username field could possibly use this issue to impersonate other users. **CVE ID : CVE-2019-3814**	N/A	O-CAN-UBUN-040419/9
Cisco					
ios_xe					
N/A	27-03-2019	6.1	A vulnerability in the Easy Virtual Switching System (VSS) of Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an unauthenticated, adjacent attacker to cause the switches to reload. The vulnerability is due to incomplete error handling when processing Cisco Discovery Protocol (CDP) packets used with the Easy Virtual Switching System. An attacker could exploit this vulnerability by sending a specially crafted CDP packet. An exploit could allow the attacker to	N/A	O-CIS-IOS_-040419/10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause the device to reload, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2019-1750**		
N/A	27-03-2019	7.8	A vulnerability in the ISDN functions of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect processing of specific values in the Q.931 information elements. An attacker could exploit this vulnerability by calling the affected device with specific Q.931 information elements being present. An exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2019-1752**	N/A	O-CIS-IOS_-040419/11
N/A	27-03-2019	9	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated but unprivileged (level 1), remote attacker to run privileged Cisco IOS commands by using the web UI. The vulnerability is due to a failure to	N/A	O-CIS-IOS_-040419/12

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate and sanitize input in Web Services Management Agent (WSMA) functions. An attacker could exploit this vulnerability by submitting a malicious payload to the affected device's web UI. A successful exploit could allow the lower-privileged attacker to execute arbitrary commands with higher privileges on the affected device. **CVE ID : CVE-2019-1753**		
N/A	27-03-2019	9	A vulnerability in the authorization subsystem of Cisco IOS XE Software could allow an authenticated but unprivileged (level 1), remote attacker to run privileged Cisco IOS commands by using the web UI. The vulnerability is due to improper validation of user privileges of web UI users. An attacker could exploit this vulnerability by submitting a malicious payload to a specific endpoint in the web UI. A successful exploit could allow the lower-privileged attacker to execute arbitrary commands with	N/A	O-CIS-IOS_-040419/13

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			higher privileges on the affected device. **CVE ID : CVE-2019-1754**		
N/A	27-03-2019	9	A vulnerability in the Web Services Management Agent (WSMA) function of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary Cisco IOS commands as a privilege level 15 user. The vulnerability occurs because the affected software improperly sanitizes user-supplied input. An attacker could exploit this vulnerability by submitting crafted HTTP requests to the targeted application. A successful exploit could allow the attacker to execute arbitrary commands on the affected device. **CVE ID : CVE-2019-1755**	N/A	O-CIS-IOS_-040419/14
N/A	27-03-2019	9	A vulnerability in Cisco IOS XE Software could allow an authenticated, remote attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability occurs	N/A	O-CIS-IOS_-040419/15

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because the affected software improperly sanitizes user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying a username with a malicious payload in the web UI and subsequently making a request to a specific endpoint in the web UI. A successful exploit could allow the attacker to run arbitrary commands as the root user, allowing complete compromise of the system. **CVE ID : CVE-2019-1756**		
N/A	27-03-2019	4.3	A vulnerability in the Cisco Smart Call Home feature of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data using an invalid certificate. The vulnerability is due to insufficient certificate validation by the affected software. An attacker could exploit this vulnerability by supplying a crafted certificate to an affected device. A successful exploit could	N/A	O-CIS-IOS_-040419/16

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to conduct man-in-the-middle attacks to decrypt confidential information on user connections to the affected software. **CVE ID : CVE-2019-1757**		
IOS					
N/A	27-03-2019	7.8	A vulnerability in the Network Address Translation 64 (NAT64) functions of Cisco IOS Software could allow an unauthenticated, remote attacker to cause either an interface queue wedge or a device reload. The vulnerability is due to the incorrect handling of certain IPv4 packet streams that are sent through the device. An attacker could exploit this vulnerability by sending specific IPv4 packet streams through the device. An exploit could allow the attacker to either cause an interface queue wedge or a device reload, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2019-1751**	N/A	O-CIS-IOS-040419/17
N/A	27-03-2019	7.8	A vulnerability in the ISDN functions of Cisco IOS Software and Cisco IOS XE Software could allow an	N/A	O-CIS-IOS-040419/18

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect processing of specific values in the Q.931 information elements. An attacker could exploit this vulnerability by calling the affected device with specific Q.931 information elements being present. An exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2019-1752**		
N/A	27-03-2019	9	A vulnerability in Cisco IOS XE Software could allow an authenticated, remote attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability occurs because the affected software improperly sanitizes user-supplied input. An attacker who has valid administrator access to an affected device could exploit this vulnerability by supplying a username with a malicious payload in the web UI and	N/A	O-CIS-IOS-040419/19

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subsequently making a request to a specific endpoint in the web UI. A successful exploit could allow the attacker to run arbitrary commands as the root user, allowing complete compromise of the system. **CVE ID : CVE-2019-1756**		
N/A	27-03-2019	4.3	A vulnerability in the Cisco Smart Call Home feature of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data using an invalid certificate. The vulnerability is due to insufficient certificate validation by the affected software. An attacker could exploit this vulnerability by supplying a crafted certificate to an affected device. A successful exploit could allow the attacker to conduct man-in-the-middle attacks to decrypt confidential information on user connections to the affected software. **CVE ID : CVE-2019-1757**	N/A	O-CIS-IOS-040419/20
Debian					
debian_linux					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	2.1	The function hso_get_config_data in drivers/net/usb/hso.c in the Linux kernel through 4.19.8 reads if_num from the USB device (as a u8) and uses it to index a small array, resulting in an object out-of-bounds (OOB) read that potentially allows arbitrary read in the kernel address space. **CVE ID : CVE-2018-19985**	N/A	O-DEB-DEBI-040419/21
N/A	21-03-2019	4.6	Yubico libu2f-host 1.1.6 contains unchecked buffers in devs.c, which could enable a malicious token to exploit a buffer overflow. An attacker could use this to attempt to execute malicious code using a crafted USB device masquerading as a security token on a computer where the affected library is currently in use. It is not possible to perform this attack with a genuine YubiKey. **CVE ID : CVE-2018-20340**	https://www.yubico.com/support/security-advisories/ysa-2019-01/	O-DEB-DEBI-040419/22
N/A	21-03-2019	9.3	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way	N/A	O-DEB-DEBI-040419/23

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3855**		
N/A	25-03-2019	6.8	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3856**	N/A	O-DEB-DEBI-040419/24
N/A	25-03-2019	6.8	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3857**	N/A	O-DEB-DEBI-040419/25

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3858**	N/A	O-DEB-DEBI-040419/26
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3859**	N/A	O-DEB-DEBI-040419/27
N/A	25-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3860**	N/A	O-DEB-DEBI-040419/28

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	25-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3861**	N/A	O-DEB-DEBI-040419/29
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3862**	N/A	O-DEB-DEBI-040419/30
N/A	25-03-2019	6.8	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out	N/A	O-DEB-DEBI-040419/31

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of bounds memory write error. **CVE ID : CVE-2019-3863**		
N/A	21-03-2019	4.6	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free. **CVE ID : CVE-2019-7221**	N/A	O-DEB-DEBI-040419/32
N/A	21-03-2019	2.1	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak. **CVE ID : CVE-2019-7222**	N/A	O-DEB-DEBI-040419/33
N/A	28-03-2019	7.2	In Dovecot before 2.2.36.3 and 2.3.x before 2.3.5.1, a local attacker can cause a buffer overflow in the indexer-worker process, which can be used to elevate to root. This occurs because of missing checks in the fts and pop3-uidl components. **CVE ID : CVE-2019-7524**	N/A	O-DEB-DEBI-040419/34
N/A	22-03-2019	7.2	rbash in Bash before 4.4-beta2 did not prevent the shell user from modifying BASH_CMDS, thus allowing the user to execute any command with the permissions of the shell. **CVE ID : CVE-2019-9924**	N/A	O-DEB-DEBI-040419/35
Dlink					
dir-816_firmware					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	25-03-2019	5	The D-Link DIR-816 A2 1.11 router only checks the random token when authorizing a goform request. An attacker can get this token from dir_login.asp and use an API URL /goform/setSysAdm to edit the web or system account without authentication. **CVE ID : CVE-2019-10039**	N/A	O-DLI-DIR--040419/36
N/A	25-03-2019	10	The D-Link DIR-816 A2 1.11 router only checks the random token when authorizing a goform request. An attacker can get this token from dir_login.asp and use a hidden API URL /goform/SystemCommand to execute a system command without authentication. **CVE ID : CVE-2019-10040**	N/A	O-DLI-DIR--040419/37
N/A	25-03-2019	5	The D-Link DIR-816 A2 1.11 router only checks the random token when authorizing a goform request. An attacker can get this token from dir_login.asp and use an API URL /goform/form2userconfig.cgi to edit the system account without	N/A	O-DLI-DIR--040419/38

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. **CVE ID : CVE-2019-10041**		
N/A	25-03-2019	7.8	The D-Link DIR-816 A2 1.11 router only checks the random token when authorizing a goform request. An attacker can get this token from dir_login.asp and use an API URL /goform/LoadDefaultSettings to reset the router without authentication. **CVE ID : CVE-2019-10042**	N/A	O-DLI-DIR--040419/39
Fedoraproject					
Fedora					
N/A	27-03-2019	5	A vulnerability was found in gnutls versions from 3.5.8 before 3.6.7. A memory corruption (double free) vulnerability in the certificate verification API. Any client or server application that verifies X.509 certificates with GnuTLS 3.5.8 or later is affected. **CVE ID : CVE-2019-3829**	N/A	O-FED-FEDO-040419/40
N/A	26-03-2019	4	A vulnerability was found in moodle before versions 3.6.3 and 3.5.5. There was a link to site home within the the Boost theme's secure layout, meaning students could navigate out of the page.	N/A	O-FED-FEDO-040419/41

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3851		
N/A	21-03-2019	9.3	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3855**	N/A	O-FED-FEDO-040419/42
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3858**	N/A	O-FED-FEDO-040419/43
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client	N/A	O-FED-FEDO-040419/44

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory. **CVE ID : CVE-2019-3859**		
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3862**	N/A	O-FED-FEDO-040419/45
N/A	21-03-2019	6.5	A vulnerability was found in PowerDNS Authoritative Server before 4.0.7 and before 4.1.7. An insufficient validation of data coming from the user when building a HTTP request from a DNS query in the HTTP Connector of the Remote backend, allowing a remote user to cause a denial of service by making the server connect to an invalid endpoint, or possibly information disclosure by making the server connect to an internal endpoint and somehow extracting meaningful information about the response	N/A	O-FED-FEDO-040419/46

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3871		
N/A	27-03-2019	4.3	A vulnerability was found in mod_auth_mellon before v0.14.2. An open redirect in the logout URL allows requests with backslashes to pass through by assuming that it is a relative URL, while the browsers silently convert backslash characters into forward slashes treating them as an absolute URL. This mismatch allows an attacker to bypass the redirect URL validation logic in apr_uri_parse function. **CVE ID : CVE-2019-3877**	N/A	O-FED-FEDO-040419/47
N/A	26-03-2019	6.8	A vulnerability was found in mod_auth_mellon before v0.14.2. If Apache is configured as a reverse proxy and mod_auth_mellon is configured to only let through authenticated users (with the require valid-user directive), adding special HTTP headers that are normally used to start the special SAML ECP (non-browser based) can be used to bypass authentication. **CVE ID : CVE-2019-3878**	N/A	O-FED-FEDO-040419/48
N/A	21-03-2019	4.6	The KVM implementation	N/A	O-FED-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the Linux kernel through 4.20.5 has a Use-after-Free. **CVE ID : CVE-2019-7221**		FEDO-040419/49
N/A	21-03-2019	2.1	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak. **CVE ID : CVE-2019-7222**	N/A	O-FED-FEDO-040419/50
ghs					
integrity_rtos					
N/A	25-03-2019	5	An issue was discovered in the Interpeak IPCOMShell TELNET server on Green Hills INTEGRITY RTOS 5.0.4. The undocumented shell command "prompt" sets the (user controlled) shell's prompt value, which is used as a format string input to printf, resulting in an information leak of memory addresses. **CVE ID : CVE-2019-7711**	N/A	O-GHS-INTE-040419/51
N/A	25-03-2019	5	An issue was discovered in handler_ipcom_shell_pwd in the Interpeak IPCOMShell TELNET server on Green Hills INTEGRITY RTOS 5.0.4. When using the pwd command, the current working directory path is used as the first argument to printf() without a proper check. An attacker	N/A	O-GHS-INTE-040419/52

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may thus forge a path containing format string modifiers to get a custom format string evaluated. This results in an information leak of memory addresses. **CVE ID : CVE-2019-7712**		
N/A	25-03-2019	7.5	An issue was discovered in the Interpeak IPCOMShell TELNET server on Green Hills INTEGRITY RTOS 5.0.4. There is a heap-based buffer overflow in the function responsible for printing the shell prompt, when a custom modifier is used to display information such as a process ID, IP address, or current working directory. Modifier expansion triggers this overflow, causing memory corruption or a crash (and also leaks memory address information). **CVE ID : CVE-2019-7713**	N/A	O-GHS-INTE-040419/53
N/A	25-03-2019	7.5	An issue was discovered in Interpeak IPWEBS on Green Hills INTEGRITY RTOS 5.0.4. It allocates 60 bytes for the HTTP Authentication header. However, when copying this header to parse, it does not check the size of	N/A	O-GHS-INTE-040419/54

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the header, leading to a stack-based buffer overflow. **CVE ID : CVE-2019-7714**		
N/A	25-03-2019	5	An issue was discovered in the Interpeak IPCOMShell TELNET server on Green Hills INTEGRITY RTOS 5.0.4. The main shell handler function uses the value of the environment variable ipcom.shell.greeting as the first argument to printf(). Setting this variable using the sysvar command results in a user-controlled format string during login, resulting in an information leak of memory addresses. **CVE ID : CVE-2019-7715**	N/A	O-GHS-INTE-040419/55
gl-inet					
gl-ar300m-lite_firmware					
N/A	21-03-2019	6.5	Command injection vulnerability in login_cgi in GL.iNet GL-AR300M-Lite devices with firmware 2.27 allows remote attackers to execute arbitrary code. **CVE ID : CVE-2019-6272**	N/A	O-GL--GL-A-040419/56
N/A	21-03-2019	4	download_file in GL.iNet GL-AR300M-Lite devices with firmware 2.27 allows remote attackers to download arbitrary files.	N/A	O-GL--GL-A-040419/57

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6273		
N/A	21-03-2019	6.5	Directory traversal vulnerability in storage_cgi in GL.iNet GL-AR300M-Lite devices with firmware 2.27 allows remote attackers to have unspecified impact via directory traversal sequences. **CVE ID : CVE-2019-6274**	N/A	O-GL--GL-A-040419/58
N/A	21-03-2019	6.5	Command injection vulnerability in firmware_cgi in GL.iNet GL-AR300M-Lite devices with firmware 2.27 allows remote attackers to execute arbitrary code. **CVE ID : CVE-2019-6275**	N/A	O-GL--GL-A-040419/59
hms-networks					
netbiter_ec150_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form. **CVE ID : CVE-2018-19694**	N/A	O-HMS-NETB-040419/60
netbiter_ec250_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form. **CVE ID : CVE-2018-19694**	N/A	O-HMS-NETB-040419/61

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
netbiter_lc310_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form. **CVE ID : CVE-2018-19694**	N/A	O-HMS-NETB-040419/62
netbiter_lc310_thingworx_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form. **CVE ID : CVE-2018-19694**	N/A	O-HMS-NETB-040419/63
netbiter_lc350_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form. **CVE ID : CVE-2018-19694**	N/A	O-HMS-NETB-040419/64
netbiter_lc350_thingworx_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form. **CVE ID : CVE-2018-19694**	N/A	O-HMS-NETB-040419/65
netbiter_ws100_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form.	N/A	O-HMS-NETB-040419/66

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-19694		
netbiter_ws200_firmware					
N/A	21-03-2019	4.3	HMS Industrial Networks Netbiter WS100 3.30.5 devices and previous have reflected XSS in the login form. **CVE ID : CVE-2018-19694**	N/A	O-HMS-NETB-040419/67
insteon					
hub_firmware					
N/A	21-03-2019	5.5	An exploitable buffer overflow vulnerability exists in the PubNub message handler Insteon Hub 2245-222 - Firmware version 1012 for the cc channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker can send an authenticated HTTP request At 0x9d014dd8 the value for the id key is copied using strcpy to the buffer at $sp+0x290. This buffer is 32 bytes large, sending anything longer will cause a buffer overflow. **CVE ID : CVE-2017-16253**	N/A	O-INS-HUB_-040419/68
N/A	21-03-2019	5.5	An exploitable buffer overflow vulnerability	N/A	O-INS-HUB_-040419/69

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exists in the PubNub message handler Insteon Hub 2245-222 - Firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker can send an authenticated HTTP request at 0x9d014e4c the value for the flg key is copied using strcpy to the buffer at $sp+0x270. This buffer is 16 bytes large, sending anything longer will cause a buffer overflow. **CVE ID : CVE-2017-16254**		
N/A	21-03-2019	5.5	An exploitable buffer overflow vulnerability exists in the PubNub message handler Insteon Hub 2245-222 - Firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker can send an authenticated HTTP request at At 0x9d014e84 the value for the cmd1 key is copied using strcpy to the buffer at $sp+0x280. This buffer is 16 bytes	N/A	O-INS-HUB_-040419/70

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			large. **CVE ID : CVE-2017-16255**		
jio					
jiofi_4g_m2s_firmware					
N/A	21-03-2019	6.1	cgi-bin/qcmap_web_cgi on JioFi 4G M2S 1.0.2 devices allows a DoS (Hang) via the mask POST parameter. **CVE ID : CVE-2019-7439**	N/A	O-JIO-JIOF-040419/71
N/A	21-03-2019	4.3	JioFi 4G M2S 1.0.2 devices have CSRF via the SSID name and Security Key field under Edit Wi-Fi Settings (aka a SetWiFi_Setting request to cgi-bin/qcmap_web_cgi). **CVE ID : CVE-2019-7440**	N/A	O-JIO-JIOF-040419/72
kaiostech					
kaios					
N/A	21-03-2019	7.1	A Denial of Service issue has been discovered in the Gecko component of KaiOS 2.5 10.05 (platform 48.0.a2) on Nokia 8810 4G devices. When a crafted web page is visited with the internal browser, the Gecko process crashes with a segfault. Successful exploitation could lead to the remote code execution on the device. **CVE ID : CVE-2019-7386**	N/A	O-KAI-KAIO-040419/73
kentix					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
multisensor-lan_firmware					
N/A	21-03-2019	7.5	Kentix MultiSensor-LAN 5.63.00 devices and previous allow Authentication Bypass via an Alternate Path or Channel. **CVE ID : CVE-2018-19783**	N/A	O-KEN-MULT-040419/74
Linux					
linux_kernel					
N/A	21-03-2019	2.1	The function hso_get_config_data in drivers/net/usb/hso.c in the Linux kernel through 4.19.8 reads if_num from the USB device (as a u8) and uses it to index a small array, resulting in an object out-of-bounds (OOB) read that potentially allows arbitrary read in the kernel address space. **CVE ID : CVE-2018-19985**	N/A	O-LIN-LINU-040419/75
N/A	21-03-2019	7.2	An issue where a provided address with access_ok() is not checked was discovered in i915_gem_execbuffer2_ioctl in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Linux kernel through 4.19.13. A local attacker can craft a malicious IOCTL function call to	N/A	O-LIN-LINU-040419/76

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwrite arbitrary kernel memory, resulting in a Denial of Service or privilege escalation. **CVE ID : CVE-2018-20669**		
N/A	27-03-2019	7.8	An issue was discovered in the hwpoison implementation in mm/memory-failure.c in the Linux kernel before 5.0.4. When soft_offline_in_use_page() runs on a thp tail page after pmd is split, an attacker can cause a denial of service (BUG). **CVE ID : CVE-2019-10124**	N/A	O-LIN-LINU-040419/77
N/A	27-03-2019	10	An issue was discovered in aio_poll() in fs/aio.c in the Linux kernel through 5.0.4. A file may be released by aio_poll_wake() if an expected event is triggered immediately (e.g., by the close of a pair of pipes) after the return of vfs_poll(), and this will cause a use-after-free. **CVE ID : CVE-2019-10125**	N/A	O-LIN-LINU-040419/78
N/A	21-03-2019	4.6	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free. **CVE ID : CVE-2019-7221**	N/A	O-LIN-LINU-040419/79
N/A	21-03-2019	2.1	The KVM implementation in the Linux kernel	N/A	O-LIN-LINU-040419/80

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 4.20.5 has an Information Leak. **CVE ID : CVE-2019-7222**		
N/A	21-03-2019	4.9	In the Linux kernel through 5.0.2, the function inotify_update_existing_watch() in fs/notify/inotify/inotify_user.c neglects to call fsnotify_put_mark() with IN_MASK_CREATE after fsnotify_find_mark(), which will cause a memory leak (aka refcount leak). Finally, this will cause a denial of service. **CVE ID : CVE-2019-9857**	N/A	O-LIN-LINU-040419/81
Nokia					
8810_4g_firmware					
N/A	21-03-2019	7.1	A Denial of Service issue has been discovered in the Gecko component of KaiOS 2.5 10.05 (platform 48.0.a2) on Nokia 8810 4G devices. When a crafted web page is visited with the internal browser, the Gecko process crashes with a segfault. Successful exploitation could lead to the remote code execution on the device. **CVE ID : CVE-2019-7386**	N/A	O-NOK-8810-040419/82
Opensuse					
leap					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-03-2019	6.8	Buffer overflow in BlockIo service for EDK II may allow an unauthenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via network access. **CVE ID : CVE-2018-12180**	https://edk2-docs.gitbooks.io/security-advisory/content/buffer-overflow-in-blockio-service-for-ram-disk.html	O-OPE-LEAP-040419/83
N/A	28-03-2019	5	Keep-alive HTTP and HTTPS connections can remain open and inactive for up to 2 minutes in Node.js 6.16.0 and earlier. Node.js 8.0.0 introduced a dedicated server.keepAliveTimeout which defaults to 5 seconds. The behavior in Node.js 6.16.0 and earlier is a potential Denial of Service (DoS) attack vector. Node.js 6.17.0 introduces server.keepAliveTimeout and the 5-second default. **CVE ID : CVE-2019-5739**	N/A	O-OPE-LEAP-040419/84
N/A	21-03-2019	4.6	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free. **CVE ID : CVE-2019-7221**	N/A	O-OPE-LEAP-040419/85
N/A	21-03-2019	2.1	The KVM implementation in the Linux kernel through 4.20.5 has an	N/A	O-OPE-LEAP-040419/86

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Leak. **CVE ID : CVE-2019-7222**		
pfizer					
symbiq_infusion_system_firmware					
N/A	23-03-2019	9	Hospira Symbiq Infusion System 3.13 and earlier allows remote authenticated users to trigger "unanticipated operations" by leveraging "elevated privileges" for an unspecified call to an incorrectly exposed function. **CVE ID : CVE-2015-3965**	N/A	O-PFI-SYMB-040419/87
Redhat					
virtualization					
N/A	25-03-2019	5.5	It was discovered that in the ovirt's REST API before version 4.3.2.1, RemoveDiskCommand is triggered as an internal command, meaning the permission validation that should be performed against the calling user is skipped. A user with low privileges (eg Basic Operations) could exploit this flaw to delete disks attached to guests. **CVE ID : CVE-2019-3879**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3879	O-RED-VIRT-040419/88
enterprise_linux					
N/A	27-03-2019	4.3	A vulnerability was found in mod_auth_mellon before	N/A	O-RED-ENTE-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v0.14.2. An open redirect in the logout URL allows requests with backslashes to pass through by assuming that it is a relative URL, while the browsers silently convert backslash characters into forward slashes treating them as an absolute URL. This mismatch allows an attacker to bypass the redirect URL validation logic in apr_uri_parse function. **CVE ID : CVE-2019-3877**		040419/89
N/A	26-03-2019	6.8	A vulnerability was found in mod_auth_mellon before v0.14.2. If Apache is configured as a reverse proxy and mod_auth_mellon is configured to only let through authenticated users (with the require valid-user directive), adding special HTTP headers that are normally used to start the special SAML ECP (non-browser based) can be used to bypass authentication. **CVE ID : CVE-2019-3878**	N/A	O-RED-ENTE-040419/90
Samsung					
galaxy_s6_firmware					
N/A	21-03-2019	5.8	Buffer overflow in prot_get_ring_space in the	https://security.samsung	O-SAM-GALA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bcmdhd4358 Wi-Fi driver on the Samsung Galaxy S6 SM-G920F G920FXXU5EQH7 allows an attacker (who has obtained code execution on the Wi-Fi chip) to overwrite kernel memory due to improper validation of the ring buffer read pointer. The Samsung ID is SVE-2018-12029. **CVE ID : CVE-2018-14745**	mobile.com/ securityUpdate.smsb	040419/91
x7400gx_firmware					
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in "/sws/swsAlert.sws" in multiple parameters: flag, frame, func, and Nfunc. **CVE ID : CVE-2019-7418**	N/A	O-SAM-X740-040419/92
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in "/sws/leftmenu.sws" in multiple parameters: ruiFw_id, ruiFw_pid, ruiFw_title. **CVE ID : CVE-2019-7419**	N/A	O-SAM-X740-040419/93
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in	N/A	O-SAM-X740-040419/94

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"/sws.application/information/networkinformationView.sws" in the tabName parameter. **CVE ID : CVE-2019-7420**		
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in "/sws.login/gnb/loginView.sws" in multiple parameters: contextpath and basedURL. **CVE ID : CVE-2019-7421**	N/A	O-SAM-X740-040419/95
teracue					
enc-400_hdmi2_firmware					
N/A	21-03-2019	10	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. The login form passes user input directly to a shell command without any kind of escaping or validation in /usr/share/www/check.lp file. An attacker is able to perform command injection using the "password" parameter in the login form. **CVE ID : CVE-2018-20218**	N/A	O-TER-ENC--040419/96
N/A	21-03-2019	9.3	An issue was discovered on Teracue ENC-400 devices with firmware	N/A	O-TER-ENC--040419/97

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.56 and below. After successful authentication, the device sends an authentication cookie to the end user such that they can access the devices web administration panel. This token is hard-coded to a string in the source code (/usr/share/www/check.lp file). By setting this cookie in a browser, an attacker is able to maintain access to every ENC-400 device without knowing the password, which results in authentication bypass. Even if a user changes the password on the device, this token is static and unchanged. **CVE ID : CVE-2018-20219**		
N/A	21-03-2019	5	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. While the web interface requires authentication before it can be interacted with, a large portion of the HTTP endpoints are missing authentication. An attacker is able to view these pages before being authenticated, and some of these pages may disclose sensitive information.	N/A	O-TER-ENC--040419/98

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-20220		
enc-400_hdmi_firmware					
N/A	21-03-2019	10	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. The login form passes user input directly to a shell command without any kind of escaping or validation in /usr/share/www/check.lp file. An attacker is able to perform command injection using the "password" parameter in the login form. **CVE ID : CVE-2018-20218**	N/A	O-TER-ENC--040419/99
N/A	21-03-2019	9.3	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. After successful authentication, the device sends an authentication cookie to the end user such that they can access the devices web administration panel. This token is hard-coded to a string in the source code (/usr/share/www/check.lp file). By setting this cookie in a browser, an attacker is able to maintain access to every ENC-400 device without knowing the password, which	N/A	O-TER-ENC--040419/100

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			results in authentication bypass. Even if a user changes the password on the device, this token is static and unchanged. **CVE ID : CVE-2018-20219**		
N/A	21-03-2019	5	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. While the web interface requires authentication before it can be interacted with, a large portion of the HTTP endpoints are missing authentication. An attacker is able to view these pages before being authenticated, and some of these pages may disclose sensitive information. **CVE ID : CVE-2018-20220**	N/A	O-TER-ENC--040419/101
enc-400_hdsdi_firmware					
N/A	21-03-2019	10	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. The login form passes user input directly to a shell command without any kind of escaping or validation in /usr/share/www/check.lp file. An attacker is able to perform command injection using the "password" parameter in	N/A	O-TER-ENC--040419/102

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the login form. **CVE ID : CVE-2018-20218**		
N/A	21-03-2019	9.3	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. After successful authentication, the device sends an authentication cookie to the end user such that they can access the devices web administration panel. This token is hard-coded to a string in the source code (/usr/share/www/check.lp file). By setting this cookie in a browser, an attacker is able to maintain access to every ENC-400 device without knowing the password, which results in authentication bypass. Even if a user changes the password on the device, this token is static and unchanged. **CVE ID : CVE-2018-20219**	N/A	O-TER-ENC--040419/103
N/A	21-03-2019	5	An issue was discovered on Teracue ENC-400 devices with firmware 2.56 and below. While the web interface requires authentication before it can be interacted with, a large portion of the HTTP endpoints are missing authentication. An attacker	N/A	O-TER-ENC--040419/104

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is able to view these pages before being authenticated, and some of these pages may disclose sensitive information. **CVE ID : CVE-2018-20220**		
wifi-soft					
unibox_firmware					
N/A	21-03-2019	9	An issue was discovered on Wifi-soft UniBox controller 0.x through 2.x devices. network/mesh/edit-nds.php is vulnerable to arbitrary file upload, allowing an attacker to upload .php files and execute code on the server with root user privileges. Authentication for accessing this component can be bypassed by using Hard coded credentials. **CVE ID : CVE-2019-3495**	N/A	O-WIF-UNIB-040419/105
N/A	21-03-2019	9	An issue was discovered on Wifi-soft UniBox controller 3.x devices. The tools/controller/diagnostic_tools_controller Diagnostic Tools Controller is vulnerable to Remote Command Execution, allowing an attacker to execute arbitrary system commands on the server with root user privileges.	N/A	O-WIF-UNIB-040419/106

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Authentication for accessing this component can be bypassed by using Hard coded credentials. **CVE ID : CVE-2019-3496**		
N/A	21-03-2019	9	An issue was discovered on Wifi-soft UniBox controller 0.x through 2.x devices. The tools/ping Ping feature of the Diagnostic Tools component is vulnerable to Remote Command Execution, allowing an attacker to execute arbitrary system commands on the server with root user privileges. Authentication for accessing this component can be bypassed by using Hard coded credentials. **CVE ID : CVE-2019-3497**	N/A	O-WIF-UNIB-040419/107
ysoft					
safeq_server_client					
N/A	21-03-2019	6.8	YSoft SafeQ Server 6 allows a replay attack. **CVE ID : CVE-2018-15498**	N/A	O-YSO-SAFE-040419/108
Zyxel					
dsl-491hnu-b10b_firmware					
N/A	21-03-2019	6.8	ZyXEL VMG3312-B10B DSL-491HNU-B1B v2 devices allow login/login-page.cgi CSRF. **CVE ID : CVE-2019-7391**	N/A	O-ZYX-DSL--040419/109

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dsl-491hnu-b1b_v2_firmware					
N/A	21-03-2019	6.8	ZyXEL VMG3312-B10B DSL-491HNU-B1B v2 devices allow login/login-page.cgi CSRF. **CVE ID : CVE-2019-7391**	N/A	O-ZYX-DSL--040419/110
Application					
advance_crowdfunding_script_project					
advance_crowdfunding_script					
N/A	21-03-2019	5	PHP Scripts Mall Advance Crowdfunding Script 2.0.3 has directory traversal via a direct request for a listing of an uploads directory such as the wp-content/uploads/2018/12 directory. **CVE ID : CVE-2018-20630**	N/A	A-ADV-ADVA-040419/111
advanced_comment_system_project					
advanced_comment_system					
N/A	21-03-2019	4.3	internal/advanced_comment_system/index.php and internal/advanced_comment_system/admin.php in Advanced Comment System, version 1.0, contain a reflected cross-site scripting vulnerability via ACS_path. A remote unauthenticated attacker could potentially exploit this vulnerability to supply malicious HTML or JavaScript code to a vulnerable web	N/A	A-ADV-ADVA-040419/112

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application, which is then reflected back to the victim and executed by the web browser. The product is discontinued. **CVE ID : CVE-2018-18845**		
amazon_affiliate_store_project					
amazon_affiliate_store					
N/A	28-03-2019	4	PHP Scripts Mall Amazon Affiliate Store 2.1.6 allows Parameter Tampering of the payment amount. **CVE ID : CVE-2019-9864**	N/A	A-AMA-AMAZ-040419/113
Apache					
karaf					
N/A	21-03-2019	4	Apache Karaf kar deployer reads .kar archives and extracts the paths from the "repository/" and "resources/" entries in the zip file. It then writes out the content of these paths to the Karaf repo and resources directories. However, it doesn't do any validation on the paths in the zip file. This means that a malicious user could craft a .kar file with ".." directory names and break out of the directories to write arbitrary content to the filesystem. This is the "Zip-slip" vulnerability - https://snyk.io/research/zip-slip-vulnerability. This	N/A	A-APA-KARA-040419/114

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is low if the Karaf process user has limited permission on the filesystem. Any Apache Karaf releases prior 4.2.3 is impacted. **CVE ID : CVE-2019-0191**		
mesos					
N/A	25-03-2019	9.3	A specifically crafted Docker image running under the root user can overwrite the init helper binary of the container runtime and/or the command executor in Apache Mesos versions pre-1.4.x, 1.4.0 to 1.4.2, 1.5.0 to 1.5.2, 1.6.0 to 1.6.1, and 1.7.0 to 1.7.1. A malicious actor can therefore gain root-level code execution on the host. **CVE ID : CVE-2019-0204**	N/A	A-APA-MESO-040419/115
jspwiki					
N/A	28-03-2019	7.8	A specially crafted url could be used to access files under the ROOT directory of the application on Apache JSPWiki 2.9.0 to 2.11.0.M2, which could be used by an attacker to obtain registered users' details. **CVE ID : CVE-2019-0225**	N/A	A-APA-JSPW-040419/116
Hadoop					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	5.8	In Apache Hadoop 2.9.0 to 2.9.1, 2.8.3 to 2.8.4, 2.7.5 to 2.7.6, KMS blocking users or granting access to users incorrectly, if the system uses non-default groups mapping mechanisms. **CVE ID : CVE-2018-11767**	N/A	A-APA-HADO-040419/117
Activemq					
N/A	28-03-2019	5	In Apache ActiveMQ 5.0.0 - 5.15.8, unmarshalling corrupt MQTT frame can lead to broker Out of Memory exception making it unresponsive. **CVE ID : CVE-2019-0222**	N/A	A-APA-ACTI-040419/118
Atlassian					
Crowd					
N/A	29-03-2019	6.8	The console login resource in Atlassian Crowd before version 3.0.2 and from version 3.1.0 before version 3.1.1 allows remote attackers, who have previously obtained a user's JSESSIONID cookie, to gain access to some of the built-in and potentially third party rest resources via a session fixation vulnerability. **CVE ID : CVE-2017-18105**	N/A	A-ATL-CROW-040419/119
N/A	29-03-2019	6	The identifier_hash for a session token in Atlassian Crowd before version 2.9.1 could potentially collide	N/A	A-ATL-CROW-040419/120

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with an identifier_hash for another user or a user in a different directory, this allows remote attackers who can authenticate to Crowd or an application using Crowd for authentication to gain access to another user's session provided they can make their identifier hash collide with another user's session identifier hash. **CVE ID : CVE-2017-18106**		
N/A	29-03-2019	6.5	The administration SMTP configuration resource in Atlassian Crowd before version 2.10.2 allows remote attackers with administration rights to execute arbitrary code via a JNDI injection. **CVE ID : CVE-2017-18108**	N/A	A-ATL-CROW-040419/121
N/A	29-03-2019	5.8	The login resource of CrowdId in Atlassian Crowd before version 3.0.2 and from version 3.1.0 before version 3.1.1 allows remote attackers to redirect users to a different website which they may use as part of performing a phishing attack via an open redirect. **CVE ID : CVE-2017-18109**	N/A	A-ATL-CROW-040419/122
N/A	29-03-2019	4	The administration backup restore resource in	N/A	A-ATL-CROW-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Atlassian Crowd before version 3.0.2 and from version 3.1.0 before version 3.1.1 allows remote attackers to read files from the filesystem via a XXE vulnerability. **CVE ID : CVE-2017-18110**		040419/123
Confluence					
N/A	25-03-2019	7.5	The WebDAV endpoint in Atlassian Confluence Server and Data Center before version 6.6.7 (the fixed version for 6.6.x), from version 6.7.0 before 6.8.5 (the fixed version for 6.8.x), and from version 6.9.0 before 6.9.3 (the fixed version for 6.9.x) allows remote attackers to send arbitrary HTTP and WebDAV requests from a Confluence Server or Data Center instance via Server-Side Request Forgery. **CVE ID : CVE-2019-3395**	N/A	A-ATL-CONF-040419/124
N/A	25-03-2019	10	The Widget Connector macro in Atlassian Confluence Server before version 6.6.12 (the fixed version for 6.6.x), from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0	N/A	A-ATL-CONF-040419/125

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 6.14.2 (the fixed version for 6.14.x), allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection. **CVE ID : CVE-2019-3396**		
baigo					
baigo_sso					
N/A	24-03-2019	6.5	baigoStudio baigoSSO v3.0.1 allows remote attackers to execute arbitrary PHP code via the first form field of a configuration screen, because this code is written to the BG_SITE_NAME field in the opt_base.inc.php file. **CVE ID : CVE-2019-10015**	N/A	A-BAI-BAIG-040419/126
basic_b2b_script_project					
basic_b2b_script					
N/A	21-03-2019	6.8	PHP Scripts Mall Basic B2B Script 2.0.9 has Cross-Site Request Forgery (CSRF) via the Edit profile feature. **CVE ID : CVE-2018-20644**	N/A	A-BAS-BASI-040419/127
N/A	21-03-2019	3.5	PHP Scripts Mall Basic B2B Script 2.0.9 has HTML injection via the First Name or Last Name field. **CVE ID : CVE-2018-20645**	N/A	A-BAS-BASI-040419/128

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	4	PHP Scripts Mall Basic B2B Script 2.0.9 has has directory traversal via a direct request for a listing of an image directory such as an uploads/ directory. **CVE ID : CVE-2018-20646**	N/A	A-BAS-BASI-040419/129
Blogengine					
blogengine.net					
N/A	21-03-2019	7.5	An issue was discovered in BlogEngine.NET through 3.3.6.0. A path traversal and Local File Inclusion vulnerability in PostList.ascx.cs can cause unauthenticated users to load a PostView.ascx component from a potentially untrusted location on the local filesystem. This is especially dangerous if an authenticated user uploads a PostView.ascx file using the file manager utility, which is currently allowed. This results in remote code execution for an authenticated user. **CVE ID : CVE-2019-6714**	N/A	A-BLO-BLOG-040419/130
bluecms_project					
bluecms					
N/A	28-03-2019	7.5	A SQL Injection issue was discovered in BlueCMS 1.6. The variable $ad_id is spliced directly in	N/A	A-BLU-BLUE-040419/131

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uploads/admin/ad.php in the admin folder, and is not wrapped in single quotes, resulting in injection around the escape of magic quotes. **CVE ID : CVE-2019-10262**		
car_rental_script_project					
car_rental_script					
N/A	21-03-2019	4	PHP Scripts Mall Car Rental Script 2.0.8 has directory traversal via a direct request for a listing of an image directory such as an images/ directory. **CVE ID : CVE-2018-20647**	N/A	A-CAR-CAR_-040419/132
centos-webpanel					
centos_web_panel					
N/A	26-03-2019	3.5	CentOS-WebPanel.com (aka CWP) CentOS Web Panel through 0.9.8.763 is vulnerable to Stored/Persistent XSS for the "Package Name" field via the add_package module parameter. **CVE ID : CVE-2019-7646**	N/A	A-CEN-CENT-040419/133
charity_donation_script_project					
charity_donation_script					
N/A	21-03-2019	5	PHP Scripts Mall Charity Donation Script readymadeb2bscript has directory traversal via a direct request for a listing of an uploads directory	N/A	A-CHA-CHAR-040419/134

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			such as the wp-content/uploads/2018/12 directory. **CVE ID : CVE-2018-20629**		
charity_foundation_script_project					
charity_foundation_script					
N/A	21-03-2019	5	PHP Scripts Mall Charity Foundation Script 1 through 3 allows directory traversal via a direct request for a listing of an uploads directory such as the wp-content/uploads/2018/12 directory. **CVE ID : CVE-2018-20628**	N/A	A-CHA-CHAR-040419/135
chartered_accountant_auditor_website_project					
chartered_accountant_auditor_website					
N/A	21-03-2019	3.5	PHP Scripts Mall Chartered Accountant : Auditor Website 2.0.1 has HTML injection via the First Name field. **CVE ID : CVE-2018-20636**	N/A	A-CHA-CHAR-040419/136
N/A	21-03-2019	4	PHP Scripts Mall Chartered Accountant : Auditor Website 2.0.1 allows remote attackers to cause a denial of service (unrecoverable blank profile) via crafted JavaScript code in the First Name and Last Name field. **CVE ID : CVE-2018-20637**	N/A	A-CHA-CHAR-040419/137

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	4	PHP Scripts Mall Chartered Accountant : Auditor Website 2.0.1 has directory traversal via a direct request for a listing of an image directory such as an assets/ directory. **CVE ID : CVE-2018-20638**	N/A	A-CHA-CHAR-040419/138
Cmsmadesimple					
cms_made_simple					
N/A	24-03-2019	4.3	CMS Made Simple 2.2.10 has XSS via the moduleinterface.php Name field, which is reachable via an "Add a new Profile" action to the File Picker. **CVE ID : CVE-2019-10017**	N/A	A-CMS-CMS_-040419/139
N/A	26-03-2019	3.5	CMS Made Simple 2.2.10 has a Self-XSS vulnerability via the Layout Design Manager "Name" field, which is reachable via a "Create a new Template" action to the Design Manager. **CVE ID : CVE-2019-10105**	N/A	A-CMS-CMS_-040419/140
N/A	26-03-2019	3.5	CMS Made Simple 2.2.10 has XSS via the 'moduleinterface.php' Name field, which is reachable via an "Add Category" action to the "Site Admin Settings - News module" section.	N/A	A-CMS-CMS_-040419/141

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10106		
N/A	26-03-2019	3.5	CMS Made Simple 2.2.10 has XSS via the myaccount.php "Email Address" field, which is reachable via the "My Preferences -> My Account" section. **CVE ID : CVE-2019-10107**	N/A	A-CMS-CMS_-040419/142
N/A	26-03-2019	6.8	An issue was discovered in CMS Made Simple 2.2.8. It is possible with the News module, through a crafted URL, to achieve unauthenticated blind time-based SQL injection via the m1_idlist parameter. **CVE ID : CVE-2019-9053**	https://www.cmsmadesimple.org/2019/03/Announcing-CMS-Made-Simple-v2.2.10-Spuzzum	A-CMS-CMS_-040419/143
N/A	26-03-2019	6.5	An issue was discovered in CMS Made Simple 2.2.8. In the module DesignManager (in the files action.admin_bulk_css.php and action.admin_bulk_template.php), with an unprivileged user with Designer permission, it is possible reach an unserialize call with a crafted value in the m1_allparms parameter, and achieve object injection.	https://www.cmsmadesimple.org/2019/03/Announcing-CMS-Made-Simple-v2.2.10-Spuzzum	A-CMS-CMS_-040419/144

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9055		
N/A	26-03-2019	6.5	An issue was discovered in CMS Made Simple 2.2.8. In the module FilePicker, it is possible to reach an unserialize call with an untrusted parameter, and achieve authenticated object injection. **CVE ID : CVE-2019-9057**	https://www.cmsmadesimple.org/2019/03/Anouncing-CMS-Made-Simple-v2.2.10-Spuzzum	A-CMS-CMS_-040419/145
N/A	26-03-2019	6.5	An issue was discovered in CMS Made Simple 2.2.8. In the administrator page admin/changegroupperm.php, it is possible to send a crafted value in the sel_groups parameter that leads to authenticated object injection. **CVE ID : CVE-2019-9058**	https://www.cmsmadesimple.org/2019/03/Anouncing-CMS-Made-Simple-v2.2.10-Spuzzum	A-CMS-CMS_-040419/146
N/A	26-03-2019	6.5	An issue was discovered in CMS Made Simple 2.2.8. It is possible, with an administrator account, to achieve command injection by modifying the path of the e-mail executable in Mail Settings, setting "sendmail" in the "Mailer" option, and launching the "Forgot your password" feature. **CVE ID : CVE-2019-9059**	https://www.cmsmadesimple.org/2019/03/Anouncing-CMS-Made-Simple-v2.2.10-Spuzzum	A-CMS-CMS_-040419/147
N/A	26-03-2019	6.5	An issue was discovered in CMS Made Simple 2.2.8. In the module	https://www.cmsmadesimple.org/20	A-CMS-CMS_-040419/148

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ModuleManager (in the file action.installmodule.php), it is possible to reach an unserialize call with untrusted input and achieve authenticated object injection by using the "install module" feature. **CVE ID : CVE-2019-9061**	19/03/Announcing-CMS-Made-Simple-v2.2.10-Spuzzum	
cobub					
razor					
N/A	29-03-2019	7.5	Western Bridge Cobub Razor 0.8.0 has a file upload vulnerability via the web/assets/swf/uploadify.php URI, as demonstrated by a .php file with the image/jpeg content type. **CVE ID : CVE-2019-10276**	N/A	A-COB-RAZO-040419/149
consumer_reviews_script_project					
consumer_reviews_script					
N/A	21-03-2019	4	PHP Scripts Mall Consumer Reviews Script 4.0.3 has directory traversal via a direct request for a listing of an uploads directory such as the wp-content/uploads/2018/12 directory. **CVE ID : CVE-2018-20626**	N/A	A-CON-CONS-040419/150
N/A	21-03-2019	3.5	PHP Scripts Mall Consumer Reviews Script	N/A	A-CON-CONS-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.0.3 has HTML injection via the search box. **CVE ID : CVE-2018-20627**		040419/151
Coreftp					
core_ftp					
N/A	22-03-2019	5	An issue was discovered in the SFTP Server component in Core FTP 2.0 Build 674. A directory traversal vulnerability exists using the SIZE command along with a \..\..\ substring, allowing an attacker to enumerate file existence based on the returned information. **CVE ID : CVE-2019-9648**	N/A	A-COR-CORE-040419/152
N/A	22-03-2019	5	An issue was discovered in the SFTP Server component in Core FTP 2.0 Build 674. Using the MDTM FTP command, a remote attacker can use a directory traversal technique (..\..\) to browse outside the root directory to determine the existence of a file on the operating system, and its last modified date. **CVE ID : CVE-2019-9649**	N/A	A-COR-CORE-040419/153
Dedecms					
Dedecms					
N/A	24-03-2019	4	In DedeCMS 5.7SP2, member/resetpassword.p	N/A	A-DED-DEDE-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hp allows remote authenticated users to reset the passwords of arbitrary users via a modified id parameter, because the key parameter is not properly validated. **CVE ID : CVE-2019-10014**		040419/154
Digium					
Asterisk					
N/A	28-03-2019	4	An Integer Signedness issue (for a return code) in the res_pjsip_sdp_rtp module in Digium Asterisk versions 15.7.1 and earlier and 16.1.1 and earlier allows remote authenticated users to crash Asterisk via a specially crafted SDP protocol violation. **CVE ID : CVE-2019-7251**	https://issues.asterisk.org/jira/browse/ASTERISK-28260	A-DIG-ASTE-040419/155
Dovecot					
Dovecot					
N/A	27-03-2019	4.9	It was discovered that Dovecot before versions 2.2.36.1 and 2.3.4.1 incorrectly handled client certificates. A remote attacker in possession of a valid certificate with an empty username field could possibly use this issue to impersonate other users.	N/A	A-DOV-DOVE-040419/156

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3814		
N/A	28-03-2019	7.2	In Dovecot before 2.2.36.3 and 2.3.x before 2.3.5.1, a local attacker can cause a buffer overflow in the indexer-worker process, which can be used to elevate to root. This occurs because of missing checks in the fts and pop3-uidl components. **CVE ID : CVE-2019-7524**	N/A	A-DOV-DOVE-040419/157
Drupal					
Drupal					
N/A	26-03-2019	3.5	In Drupal 7 versions prior to 7.65; Drupal 8.6 versions prior to 8.6.13;Drupal 8.5 versions prior to 8.5.14. Under certain circumstances the File module/subsystem allows a malicious user to upload a file that can trigger a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2019-6341**	https://www.drupal.org/sa-core-2019-004	A-DRU-DRUP-040419/158
Eclipse					
mosquitto					
N/A	27-03-2019	5	In Eclipse Mosquitto version from 1.0 to 1.4.15, a Null Dereference vulnerability was found in the Mosquitto library which could lead to crashes for those	https://bugs.eclipse.org/bugs/show_bug.cgi?id=533775	A-ECL-MOSQ-040419/159

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			applications using the library. **CVE ID : CVE-2017-7655**		
N/A	27-03-2019	4	In Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) when a client publishes a retained message to a topic, then has its access to that topic revoked, the retained message will still be published to clients that subscribe to that topic in the future. In some applications this may result in clients being able cause effects that would otherwise not be allowed. **CVE ID : CVE-2018-12546**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=543127	A-ECL-MOSQ-040419/160
N/A	27-03-2019	6.8	When Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) is configured to use an ACL file, and that ACL file is empty, or contains only comments or blank lines, then Mosquitto will treat this as though no ACL file has been defined and use a default allow policy. The new behaviour is to have an empty ACL file mean that all access is denied, which is not a useful configuration but is not unexpected. **CVE ID : CVE-2018-12550**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=541870	A-ECL-MOSQ-040419/161

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-03-2019	6.8	When Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) is configured to use a password file for authentication, any malformed data in the password file will be treated as valid. This typically means that the malformed data becomes a username and no password. If this occurs, clients can circumvent authentication and get access to the broker by using the malformed username. In particular, a blank line will be treated as a valid empty username. Other security measures are unaffected. Users who have only used the mosquitto_passwd utility to create and modify their password files are unaffected by this vulnerability. **CVE ID : CVE-2018-12551**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=543401	A-ECL-MOSQ-040419/162
Jetty					
N/A	27-03-2019	5	In Eclipse Jetty version 9.3.x and 9.4.x, the server is vulnerable to Denial of Service conditions if a remote client sends either large SETTINGs frames container containing many settings, or many small SETTINGs frames. The	https://bugs.eclipse.org/bugs/show_bug.cgi?id=538096	A-ECL-JETT-040419/163

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to the additional CPU and memory allocations required to handle changed settings. **CVE ID : CVE-2018-12545**		
Elastic					
elasticsearch					
N/A	25-03-2019	6.8	A permission issue was found in Elasticsearch versions before 5.6.15 and 6.6.1 when Field Level Security and Document Level Security are disabled and the _aliases, _shrink, or _split endpoints are used . If the elasticsearch.yml file has xpack.security.dls_fls.enabled set to false, certain permission checks are skipped when users perform one of the actions mentioned above, to make existing data available under a new index/alias name. This could result in an attacker gaining additional permissions against a restricted index. **CVE ID : CVE-2019-7611**	N/A	A-ELA-ELAS-040419/164
entrepreneur_job_portal_script_project					
entrepreneur_job_portal_script					
N/A	21-03-2019	4.3	PHP Scripts Mall Entrepreneur Job Portal Script 3.0.1 has HTML	N/A	A-ENT-ENTR-040419/165

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection via the Search Bar. **CVE ID : CVE-2018-20639**		
N/A	21-03-2019	3.5	PHP Scripts Mall Entrepreneur Job Portal Script 3.0.1 has stored Cross-Site Scripting (XSS) via the Full Name field. **CVE ID : CVE-2018-20640**	N/A	A-ENT-ENTR-040419/166
N/A	21-03-2019	6.8	PHP Scripts Mall Entrepreneur Job Portal Script 3.0.1 has Cross-Site Request Forgery (CSRF) via the Edit Profile feature. **CVE ID : CVE-2018-20641**	N/A	A-ENT-ENTR-040419/167
N/A	21-03-2019	4	PHP Scripts Mall Entrepreneur Job Portal Script 3.0.1 allows remote attackers to cause a denial of service (outage of profile editing) via crafted JavaScript code in the KeySkills field. **CVE ID : CVE-2018-20642**	N/A	A-ENT-ENTR-040419/168
N/A	21-03-2019	4	PHP Scripts Mall Entrepreneur Job Portal Script 3.0.1 has directory traversal via a direct request for a listing of an image directory such as an assets/ directory. **CVE ID : CVE-2018-20643**	N/A	A-ENT-ENTR-040419/169
envoy					
passport					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	2.1	Envoy Passport for Android and Envoy Passport for iPhone could allow a local attacker to obtain sensitive information, caused by the storing of hardcoded OAuth Creds in plaintext. An attacker could exploit this vulnerability to obtain sensitive information. **CVE ID : CVE-2018-17500**	N/A	A-ENV-PASS-040419/170
Ericsson					
active_library_explorer					
N/A	21-03-2019	4.3	XSS exists in Ericsson Active Library Explorer (ALEX) 14.3 in multiple parameters in the "/cgi-bin/alexserv" servlet, as demonstrated by the DB, FN, fn, or id parameter. **CVE ID : CVE-2019-7417**	N/A	A-ERI-ACTI-040419/171
Faststone					
image_viewer					
N/A	26-03-2019	4.3	FastStone Image Viewer 6.5 has a User Mode Write AV starting at image00400000+0x00000000000e1237 via a crafted image file. **CVE ID : CVE-2018-15813**	N/A	A-FAS-IMAG-040419/172
N/A	26-03-2019	4.3	FastStone Image Viewer 6.5 has a User Mode Write AV starting at image00400000+0x00000	N/A	A-FAS-IMAG-040419/173

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			000001cb509 via a crafted image file. **CVE ID : CVE-2018-15814**		
N/A	26-03-2019	4.3	FastStone Image Viewer 6.5 has an Exception Handler Chain Corrupted issue starting at image00400000+0x00000000003ef68a via a crafted image file. **CVE ID : CVE-2018-15815**	N/A	A-FAS-IMAG-040419/174
N/A	26-03-2019	4.3	FastStone Image Viewer 6.5 has a Read Access Violation on Block Data Move starting at image00400000+0x0000000000002d7d via a crafted image file. **CVE ID : CVE-2018-15816**	N/A	A-FAS-IMAG-040419/175
N/A	26-03-2019	4.3	FastStone Image Viewer 6.5 has a Read Access Violation on Block Data Move starting at image00400000+0x0000000000002d63 via a crafted image file. **CVE ID : CVE-2018-15817**	N/A	A-FAS-IMAG-040419/176
Fatek					
automation_fv_designer					
N/A	21-03-2019	5	A malicious attacker can trigger a remote buffer overflow in the Communication Server in Fatek Automation PM Designer V3 Version	N/A	A-FAT-AUTO-040419/177

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.1.2.2, and Automation FV Designer Version 1.2.8.0. **CVE ID : CVE-2016-5800**		
automation_pm_designer_v3					
N/A	21-03-2019	5	A malicious attacker can trigger a remote buffer overflow in the Communication Server in Fatek Automation PM Designer V3 Version 2.1.2.2, and Automation FV Designer Version 1.2.8.0. **CVE ID : CVE-2016-5800**	N/A	A-FAT-AUTO-040419/178
Flatcore					
Flatcore					
N/A	30-03-2019	6.5	An issue was discovered in flatCore 1.4.7. acp/acp.php allows remote authenticated administrators to upload arbitrary .php files, related to the addons feature. **CVE ID : CVE-2019-10652**	N/A	A-FLA-FLAT-040419/179
Flatpak					
Flatpak					
N/A	26-03-2019	7.5	Flatpak before 1.0.8, 1.1.x and 1.2.x before 1.2.4, and 1.3.x before 1.3.1 allows a sandbox bypass. Flatpak versions since 0.8.1 address CVE-2017-5226 by using a seccomp filter to prevent sandboxed apps from using the TIOCSTI ioctl, which could	N/A	A-FLA-FLAT-040419/180

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			otherwise be used to inject commands into the controlling terminal so that they would be executed outside the sandbox after the sandboxed app exits. This fix was incomplete: on 64-bit platforms, the seccomp filter could be bypassed by an ioctl request number that has TIOCSTI in its 32 least significant bits and an arbitrary nonzero value in its 32 most significant bits, which the Linux kernel would treat as equivalent to TIOCSTI. **CVE ID : CVE-2019-10063**		
flexera					
flexnet_publisher					
N/A	21-03-2019	5	A Denial of Service vulnerability related to preemptive item deletion in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down.	https://secuniaresearch.flexerasoftware.com/advisories/85979/	A-FLE-FLEX-040419/181

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-20031		
N/A	21-03-2019	5	A Denial of Service vulnerability related to message decoding in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. **CVE ID : CVE-2018-20032**	https://secuniaresearch.flexerasoftware.com/advisories/85979/	A-FLE-FLEX-040419/182
N/A	21-03-2019	5	A Denial of Service vulnerability related to adding an item to a list in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. **CVE ID : CVE-2018-20034**	https://secuniaresearch.flexerasoftware.com/advisories/85979/	A-FLE-FLEX-040419/183
Fortinet					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fortiportal					
N/A	25-03-2019	4.3	A Cross-Site Scripting vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to execute unauthorized code or commands via the applicationSearch parameter in the FortiView functionality. **CVE ID : CVE-2017-7340**	https://fortiguard.com/psirt/FG-IR-17-114	A-FOR-FORT-040419/184
N/A	25-03-2019	7.5	A weak password recovery process vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to execute unauthorized code or commands via a hidden Close button **CVE ID : CVE-2017-7342**	https://fortiguard.com/psirt/FG-IR-17-114	A-FOR-FORT-040419/185
Freedesktop					
Poppler					
N/A	21-03-2019	4.3	PDFDoc::markObject in PDFDoc.cc in Poppler 0.74.0 mishandles dict marking, leading to stack consumption in the function Dict::find() located at Dict.cc, which can (for example) be triggered by passing a crafted pdf file to the pdfunite binary. **CVE ID : CVE-2019-9903**	N/A	A-FRE-POPP-040419/186

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
getcujo					
smart_firewall					
N/A	21-03-2019	7.2	An exploitable vulnerability exists in the verified boot protection of the CUJO Smart Firewall. It is possible to add arbitrary shell commands into the dhcpd.conf file, that persist across reboots and firmware updates, and thus allow for executing unverified commands. To trigger this vulnerability, a local attacker needs to be able to write into /config/dhcpd.conf. **CVE ID : CVE-2018-3969**	N/A	A-GET-SMAR-040419/187
N/A	21-03-2019	7.5	An exploitable double free vulnerability exists in the mdnscap binary of the CUJO Smart Firewall. When parsing mDNS packets, a memory space is freed twice if an invalid query name is encountered, leading to arbitrary code execution in the context of the mdnscap process. An unauthenticated attacker can send an mDNS message to trigger this vulnerability. **CVE ID : CVE-2018-3985**	N/A	A-GET-SMAR-040419/188
N/A	21-03-2019	7.5	An exploitable heap overflow vulnerability	N/A	A-GET-SMAR-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exists in the mdnscap binary of the CUJO Smart Firewall running firmware 7003. The string lengths are handled incorrectly when parsing character strings in mDNS resource records, leading to arbitrary code execution in the context of the mdnscap process. An unauthenticated attacker can send an mDNS message to trigger this vulnerability. **CVE ID : CVE-2018-4003**		040419/189
N/A	21-03-2019	5	An exploitable integer underflow vulnerability exists in the mdnscap binary of the CUJO Smart Firewall, version 7003. When parsing SRV records in an mDNS packet, the "RDLENGTH" value is handled incorrectly, leading to an out-of-bounds access that crashes the mdnscap process. An unauthenticated attacker can send an mDNS message to trigger this vulnerability. **CVE ID : CVE-2018-4011**	N/A	A-GET-SMAR-040419/190
N/A	21-03-2019	5	An exploitable vulnerability exists the safe browsing function of the CUJO Smart Firewall,	N/A	A-GET-SMAR-040419/191

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 7003. The bug lies in the way the safe browsing function parses HTTP requests. The "Host" header is incorrectly extracted from captured HTTP requests, which would allow an attacker to visit any malicious websites and bypass the firewall. An attacker could send an HTTP request to exploit this vulnerability. **CVE ID : CVE-2018-4030**		
Gforge					
advanced_server					
N/A	24-03-2019	4.3	GForge Advanced Server 6.4.4 allows XSS via the commonsearch.php words parameter, as demonstrated by a snippet/search/?words= substring. **CVE ID : CVE-2019-10016**	N/A	A-GFO-ADVA-040419/192
Github					
github					
N/A	28-03-2019	7.5	The Management Console in GitHub Enterprise 2.8.x before 2.8.7 has a deserialization issue that allows unauthenticated remote attackers to execute arbitrary code. This occurs because the enterprise session secret is always the same, and can	N/A	A-GIT-GITH-040419/193

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be found in the product's source code. By sending a crafted cookie signed with this secret, one can call Marshal.load with arbitrary data, which is a problem because the Marshal data format allows Ruby objects. **CVE ID : CVE-2017-18365**		
Gitlab					
Gitlab					
N/A	26-03-2019	5	GitLab CE/EE before 11.3.12, 11.4.x before 11.4.10, and 11.5.x before 11.5.3 allows Directory Traversal in Templates API. **CVE ID : CVE-2018-19856**	N/A	A-GIT-GITL-040419/194
N/A	28-03-2019	5	GitLab Community and Enterprise Edition 11.x before 11.3.13, 11.4.x before 11.4.11, and 11.5.x before 11.5.4 has Incorrect Access Control. **CVE ID : CVE-2018-20144**	N/A	A-GIT-GITL-040419/195
N/A	25-03-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.4. It allows Directory Traversal. **CVE ID : CVE-2019-6240**	N/A	A-GIT-GITL-040419/196
givewp					
give					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	4.3	The "Donation Plugin and Fundraising Platform" plugin before 2.3.1 for WordPress has wp-admin/edit.php csv XSS. **CVE ID : CVE-2019-9909**	N/A	A-GIV-GIVE-040419/197
Gnome					
gvfs					
N/A	25-03-2019	3.3	An incorrect permission check in the admin backend in gvfs before version 1.39.4 was found that allows reading and modify arbitrary files by privileged users without asking for password when no authentication agent is running. This vulnerability can be exploited by malicious programs running under privileges of users belonging to the wheel group to further escalate its privileges by modifying system files without user's knowledge. Successful exploitation requires uncommon system configuration. **CVE ID : CVE-2019-3827**	https://gitlab.gnome.org/GNOME/gvfs/merge_requests/31	A-GNO-GVFS-040419/198
GNU					
Bash					
N/A	22-03-2019	7.2	rbash in Bash before 4.4-beta2 did not prevent the shell user from modifying BASH_CMDS, thus allowing	N/A	A-GNU-BASH-040419/199

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the user to execute any command with the permissions of the shell. **CVE ID : CVE-2019-9924**		
TAR					
N/A	22-03-2019	5	pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers. **CVE ID : CVE-2019-9923**	N/A	A-GNU-TAR-040419/200
Gnutls					
N/A	27-03-2019	5	A vulnerability was found in gnutls versions from 3.5.8 before 3.6.7. A memory corruption (double free) vulnerability in the certificate verification API. Any client or server application that verifies X.509 certificates with GnuTLS 3.5.8 or later is affected. **CVE ID : CVE-2019-3829**	N/A	A-GNU-GNUT-040419/201
Graphviz					
Graphviz					
N/A	21-03-2019	4.3	An issue was discovered in lib\cdt\dttree.c in libcdt.a in graphviz 2.40.1. Stack consumption occurs because of recursive agclose calls in lib\cgraph\graph.c in	N/A	A-GRA-GRAP-040419/202

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			libcgraph.a, related to agfstsubg in lib\cgraph\subg.c. **CVE ID : CVE-2019-9904**		
Harmistechnology					
je_messenger					
N/A	29-03-2019	6.4	An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. Input does not get validated and queries are not written in a way to prevent SQL injection. Therefore arbitrary SQL-Statements can be executed in the database. **CVE ID : CVE-2019-9918**	N/A	A-HAR-JE_M-040419/203
N/A	29-03-2019	3.5	An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. It is possible to craft messages in a way that JavaScript gets executed on the side of the receiving user when the message is opened, aka XSS. **CVE ID : CVE-2019-9919**	N/A	A-HAR-JE_M-040419/204
N/A	29-03-2019	6.5	An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. It is possible to perform an action within the context of the account of another user.	N/A	A-HAR-JE_M-040419/205

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9920		
N/A	29-03-2019	4	An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. It is possible to read information that should only be accessible by a different user. **CVE ID : CVE-2019-9921**	N/A	A-HAR-JE_M-040419/206
N/A	29-03-2019	5	An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. Directory Traversal allows read access to arbitrary files. **CVE ID : CVE-2019-9922**	N/A	A-HAR-JE_M-040419/207
hashicorp					
consul					
N/A	26-03-2019	5.8	HashiCorp Consul 1.4.3 lacks server hostname verification for agent-to-agent TLS communication. In other words, the product behaves as if verify_server_hostname were set to false, even when it is actually set to true. This is fixed in 1.4.4. **CVE ID : CVE-2019-9764**	N/A	A-HAS-CONS-040419/208
heimdalsecurity					
thor					
N/A	21-03-2019	6.4	Heimdal Thor Agent 2.5.17x before 2.5.173 does not verify X.509 certificates from TLS	N/A	A-HEI-THOR-040419/209

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			servers, which allows remote attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2019-8351**		
hivewebstudios					
font_organizer					
N/A	21-03-2019	4.3	The font-organizer plugin 2.1.1 for WordPress has wp-admin/options-general.php manage_font_id XSS. **CVE ID : CVE-2019-9908**	N/A	A-HIV-FONT-040419/210
Hospira					
Mednet					
N/A	26-03-2019	10	Hospira MedNet software version 5.8 and prior uses vulnerable versions of the JBoss Enterprise Application Platform software that may allow unauthenticated users to execute arbitrary code on the target system. Hospira has developed a new version of the MedNet software, MedNet 6.1. Existing versions of MedNet can be upgraded to MedNet 6.1. **CVE ID : CVE-2014-5401**	N/A	A-HOS-MEDN-040419/211
HP					
isaac_mizrahi_smartwatch					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-03-2019	5	A potential security vulnerability caused by the use of insecure (http) transactions during login has been identified with early versions of the Isaac Mizrahi Smartwatch mobile app. HP has no access to customer data as a result of this issue. **CVE ID : CVE-2017-2748**	https://support.hp.com/us-en/document/c05976868	A-HP-ISAA-040419/212
tommy_hilfiger_th24/7					
N/A	27-03-2019	2.1	A potential security vulnerability caused by incomplete obfuscation of application configuration information was discovered in Tommy Hilfiger TH24/7 Android app versions 2.0.0.11, 2.0.1.14, 2.1.0.16, and 2.2.0.19. HP has no access to customer data as a result of this issue. **CVE ID : CVE-2017-2752**	https://support.hp.com/us-en/document/c05904705	A-HP-TOMM-040419/213
synaptics_touchpad_driver					
N/A	21-03-2019	2.1	SynTP.sys in Synaptics Touchpad drivers before 2018-06-06 allows local users to obtain sensitive information about freed kernel addresses. **CVE ID : CVE-2018-15532**	https://www.synaptics.com/sites/default/files/touchpad-driver-security-brief-20190124.pdf	A-HP-SYNA-040419/214

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
remote_graphics_software					
N/A	27-03-2019	6.4	A potential vulnerability has been identified in HP Remote Graphics Software?s certificate authentication process version 7.5.0 and earlier. **CVE ID : CVE-2018-5926**	https://support.hp.com/us-en/document/c06201418	A-HP-REMO-040419/215
support_assistant					
N/A	27-03-2019	4.1	HP Support Assistant before 8.7.50.3 allows an unauthorized person with local access to load arbitrary code. **CVE ID : CVE-2018-5927**	https://support.hp.com/us-en/document/c06242762	A-HP-SUPP-040419/216
arcsight_logger					
N/A	25-03-2019	7.5	Mitigates a potential remote code execution issue in ArcSight Logger versions prior to 6.7. **CVE ID : CVE-2019-3479**	N/A	A-HP-ARCS-040419/217
N/A	25-03-2019	4.3	Mitigates a stored/reflected XSS issue in ArcSight Logger versions prior to 6.7. **CVE ID : CVE-2019-3480**	N/A	A-HP-ARCS-040419/218
N/A	25-03-2019	7.5	Mitigates a XML External Entity Parsing issue in ArcSight Logger versions prior to 6.7. **CVE ID : CVE-2019-3481**	N/A	A-HP-ARCS-040419/219
N/A	25-03-2019	6.8	Mitigates a directory traversal issue in ArcSight Logger versions prior to	N/A	A-HP-ARCS-040419/220

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.7. **CVE ID : CVE-2019-3482**		
N/A	25-03-2019	6.8	Mitigates a potential information leakage issue in ArcSight Logger versions prior to 6.7. **CVE ID : CVE-2019-3483**	N/A	A-HP-ARCS-040419/221
N/A	25-03-2019	7.2	Mitigates a remote code execution issue in ArcSight Logger versions prior to 6.7. **CVE ID : CVE-2019-3484**	N/A	A-HP-ARCS-040419/222
Humhub					
Humhub					
N/A	21-03-2019	4.3	A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in file/file/upload in Humhub 1.3.10 Community Edition. The user-supplied input containing a JavaScript payload in the filename parameter is echoed back, which resulted in reflected XSS. **CVE ID : CVE-2019-9093**	N/A	A-HUM-HUMH-040419/223
N/A	21-03-2019	4.3	A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in /s/adada/cfiles/upload in Humhub 1.3.10 Community Edition. The	N/A	A-HUM-HUMH-040419/224

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input containing JavaScript in the filename is echoed back in JavaScript code, which resulted in XSS. **CVE ID : CVE-2019-9094**		
hyphp					
hybbs					
N/A	29-03-2019	6.8	An issue was discovered in HYBBS 2.2. /?admin/user.html has a CSRF vulnerability that can add an administrator account. **CVE ID : CVE-2019-10644**	N/A	A-HYP-HYBB-040419/225
IBM					
api_connect					
N/A	22-03-2019	5	IBM API Connect 2018.1 and 2018.4.1.2 apis can be leveraged by unauthenticated users to discover login ids of registered users. IBM X-Force ID: 156544. **CVE ID : CVE-2019-4052**	N/A	A-IBM-API_-040419/226
websphere_application_server					
N/A	25-03-2019	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by improper handling of request headers. A remote attacker could exploit this vulnerability to cause the	https://www.ibm.com/support/docview.wss?uid=ibm10869570	A-IBM-WEBS-040419/227

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			consumption of Memory. IBM X-Force ID: 156242. **CVE ID : CVE-2019-4046**		
content_navigator					
N/A	22-03-2019	6.4	IBM Content Navigator 3.0CD could allow attackers to direct web traffic to a malicious site. If attackers make a fake IBM Content Navigator site, they can send a link to ICN users to send request to their Edit client directly. Then Edit client will download documents from the fake ICN website. IBM X-Force ID: 156001. **CVE ID : CVE-2019-4035**	N/A	A-IBM-CONT-040419/228
DB2					
N/A	21-03-2019	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 binaries load shared libraries from an untrusted path potentially giving low privilege user full access to root by loading a malicious shared library. IBM X-Force ID: 158014. **CVE ID : CVE-2019-4094**	https://www.ibm.com/support/docview.wss?uid=ibm10875860	A-IBM-DB2-040419/229
Imagemagick					
Imagemagick					
N/A	30-03-2019	4.3	In ImageMagick 7.0.8-36	N/A	A-IMA-IMAG-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Q16, there is a memory leak in the function SVGKeyValuePairs of coders/svg.c, which allows an attacker to cause a denial of service via a crafted image file. **CVE ID : CVE-2019-10649**		040419/230
N/A	30-03-2019	5.8	In ImageMagick 7.0.8-36 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or information disclosure via a crafted image file. **CVE ID : CVE-2019-10650**	N/A	A-IMA-IMAG-040419/231
N/A	23-03-2019	6.8	In ImageMagick 7.0.8-35 Q16, there is a stack-based buffer overflow in the function PopHexPixel of coders/ps.c, which allows an attacker to cause a denial of service or code execution via a crafted image file. **CVE ID : CVE-2019-9956**	N/A	A-IMA-IMAG-040419/232
invoiceplane					
invoiceplane					
N/A	21-03-2019	3.5	InvoicePlane 1.5 has stored XSS via the index.php/invoices/ajax/save invoice_password parameter, aka the "PDF password" field to the	N/A	A-INV-INVO-040419/233

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"Create Invoice" option. The XSS payload is rendered at an index.php/invoices/view/## URI. NOTE: this is different from CVE-2018-12255. **CVE ID : CVE-2019-7223**		
Iobit					
smart_defrag					
N/A	21-03-2019	2.1	SmartDefragDriver.sys (2.0) in IObit Smart Defrag 6 never frees an executable kernel pool that is allocated with user defined bytes and size when IOCTL 0x9C401CC4 is called. This kernel pointer can be leaked if the kernel pool becomes a "big" pool. **CVE ID : CVE-2019-6492**	N/A	A-IOB-SMAR-040419/234
ipycache_project					
ipycache					
N/A	21-03-2019	6.8	A code injection issue was discovered in ipycache through 2016-05-31. **CVE ID : CVE-2019-7539**	https://github.com/rossant/ipycache/issues/47	A-IPY-IPYC-040419/235
Jenkins					
script_security					
N/A	28-03-2019	7.5	A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.55 and earlier allows attackers to invoke	N/A	A-JEN-SCRI-040419/236

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary constructors in sandboxed scripts. **CVE ID : CVE-2019-1003040**		
pipeline_groovy					
N/A	28-03-2019	7.5	A sandbox bypass vulnerability in Jenkins Pipeline: Groovy Plugin 2.64 and earlier allows attackers to invoke arbitrary constructors in sandboxed scripts. **CVE ID : CVE-2019-1003041**	N/A	A-JEN-PIPE-040419/237
lockable_resources					
N/A	28-03-2019	3.5	A cross site scripting vulnerability in Jenkins Lockable Resources Plugin 2.4 and earlier allows attackers able to control resource names to inject arbitrary JavaScript in web pages rendered by the plugin. **CVE ID : CVE-2019-1003042**	N/A	A-JEN-LOCK-040419/238
fortify_on_demand_uploader					
N/A	28-03-2019	4.3	A cross-site request forgery vulnerability in Jenkins Fortify on Demand Uploader Plugin 3.0.10 and earlier allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-**	N/A	A-JEN-FORT-040419/239

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1003046		
N/A	28-03-2019	4	A missing permission check in Jenkins Fortify on Demand Uploader Plugin 3.0.10 and earlier allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003047**	N/A	A-JEN-FORT-040419/240
prqa					
N/A	28-03-2019	2.1	A vulnerability in Jenkins PRQA Plugin 3.1.0 and earlier allows attackers with local file system access to the Jenkins home directory to obtain the unencrypted password from the plugin configuration. **CVE ID : CVE-2019-1003048**	N/A	A-JEN-PRQA-040419/241
jenzabar					
internet_campus_solution					
N/A	25-03-2019	6	Jenzabar JICS (aka Internet Campus Solution) before 9 allows remote attackers to upload and execute arbitrary .aspx code by placing it in a ZIP archive and using the Moxie Manager plugin before 2.1.4 in the ICS\ICS.NET\ICSFileServer	N/A	A-JEN-INTE-040419/242

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/moxiemanager directory. **CVE ID : CVE-2019-10012**		
king-theme					
kingcomposer					
N/A	21-03-2019	4.3	The kingcomposer plugin 2.7.6 for WordPress has wp-admin/admin.php?page=kc-mapper id XSS. **CVE ID : CVE-2019-9910**	N/A	A-KIN-KING-040419/243
Laravel					
framework					
N/A	28-03-2019	6.5	Laravel 5.4.15 is vulnerable to Error based SQL injection in save.php via dhx_user and dhx_version parameters. **CVE ID : CVE-2018-6330**	N/A	A-LAR-FRAM-040419/244
lcds					
laquis_scada					
N/A	27-03-2019	6.8	Opening a specially crafted LCDS LAquis SCADA before 4.3.1.71 ELS file may result in a write past the end of an allocated buffer, which may allow an attacker to execute remote code in the context of the current process. **CVE ID : CVE-2019-6536**	N/A	A-LCD-LAQU-040419/245
librenms					
librenms					
N/A	28-03-2019	6.5	LibreNMS through 1.47	N/A	A-LIB-LIBR-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows SQL injection via the html/ajax_table.php sort[hostname] parameter, exploitable by authenticated users during a search. **CVE ID : CVE-2018-20678**		040419/246
Libreoffice					
Libreoffice					
N/A	25-03-2019	6.8	It was found that libreoffice before versions 6.0.7 and 6.1.3 was vulnerable to a directory traversal attack which could be used to execute arbitrary macros bundled with a document. An attacker could craft a document, which when opened by LibreOffice, would execute a Python method from a script in any arbitrary file system location, specified relative to the LibreOffice install location. **CVE ID : CVE-2018-16858**	N/A	A-LIB-LIBR-040419/247
libseccomp_project					
libseccomp					
N/A	21-03-2019	7.5	libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might able to lead to bypassing	N/A	A-LIB-LIBS-040419/248

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			seccomp filters and potential privilege escalations. **CVE ID : CVE-2019-9893**		
libsndfile_project					
libsndfile					
N/A	21-03-2019	1.9	It was discovered the fix for CVE-2018-19758 (libsndfile) was not complete and still allows a read beyond the limits of a buffer in wav_write_header() function in wav.c. A local attacker may use this flaw to make the application crash. **CVE ID : CVE-2019-3832**	https://github.com/erikd/libsndfile/pull/460	A-LIB-LIBS-040419/249
Libssh2					
Libssh2					
N/A	21-03-2019	9.3	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3855**	N/A	A-LIB-LIBS-040419/250
N/A	25-03-2019	6.8	An integer overflow flaw, which could lead to an out	N/A	A-LIB-LIBS-040419/251

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3856**		
N/A	25-03-2019	6.8	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3857**	N/A	A-LIB-LIBS-040419/252
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	N/A	A-LIB-LIBS-040419/253

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3858		
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3859**	N/A	A-LIB-LIBS-040419/254
N/A	25-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3860**	N/A	A-LIB-LIBS-040419/255
N/A	25-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	N/A	A-LIB-LIBS-040419/256

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3861		
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3862**	N/A	A-LIB-LIBS-040419/257
N/A	25-03-2019	6.8	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error. **CVE ID : CVE-2019-3863**	N/A	A-LIB-LIBS-040419/258
localhost-now_project					
localhost-now					
N/A	21-03-2019	5	A path traversal vulnerability in localhost-now npm package version 1.0.2 allows the attackers to read content of arbitrary files on the	N/A	A-LOC-LOCA-040419/259

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote server. **CVE ID : CVE-2019-5416**		
mailcleaner					
mailcleaner					
N/A	21-03-2019	9	www/soap/application/MCSoap/Logs.php in MailCleaner Community Edition 2018.08 allows remote attackers to execute arbitrary OS commands. **CVE ID : CVE-2018-20323**	N/A	A-MAI-MAIL-040419/260
Microfocus					
netiq_edirectory					
N/A	21-03-2019	5	NetIQ eDirectory versions prior to 9.0.2, under some circumstances, could be susceptible to downgrade of communication security. **CVE ID : CVE-2016-9166**	https://www.netiq.com/documentation/edirectory-9/edirectory902_releasenotes/data/edirectory902_releasenotes.html	A-MIC-NETI-040419/261
solutions_business_manager					
N/A	27-03-2019	7.5	Unauthenticated remote code execution issue in Micro Focus Solutions Business Manager (SBM) (formerly Serena Business Manager (SBM)) versions prior to 11.5. **CVE ID : CVE-2018-19641**	http://help.serena.com/doc_center/sbm/ver11_5/sbm_release_notes.htm	A-MIC-SOLU-040419/262

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-03-2019	5	Denial of service issue in Micro Focus Solutions Business Manager (SBM) (formerly Serena Business Manager (SBM)) versions prior to 11.5. **CVE ID : CVE-2018-19642**	http://help.serena.com/doc_center/sbm/ver11_5/sbm_release_notes.htm	A-MIC-SOLU-040419/263
N/A	27-03-2019	5	Information leakage issue in Micro Focus Solutions Business Manager (SBM) (formerly Serena Business Manager (SBM)) versions prior to 11.5. **CVE ID : CVE-2018-19643**	http://help.serena.com/doc_center/sbm/ver11_5/sbm_release_notes.htm	A-MIC-SOLU-040419/264
N/A	27-03-2019	4.3	Reflected cross site script issue in Micro Focus Solutions Business Manager (SBM) (formerly Serena Business Manager (SBM)) versions prior to 11.5. **CVE ID : CVE-2018-19644**	http://help.serena.com/doc_center/sbm/ver11_5/sbm_release_notes.htm	A-MIC-SOLU-040419/265
data_protector					
N/A	25-03-2019	7.5	Remote arbitrary code execution in Micro Focus Data Protector, version 10.03 this vulnerability could allow remote arbitrary code execution. **CVE ID : CVE-2019-3476**	N/A	A-MIC-DATA-040419/266
Misp					
Misp					
N/A	28-03-2019	4.3	In MISP before 2.4.105, the app/View/Layouts/default.ctp default layout	N/A	A-MIS-MISP-040419/267

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template has a Reflected XSS vulnerability. **CVE ID : CVE-2019-10254**		
Moodle					
Moodle					
N/A	25-03-2019	4	A flaw was found in Moodle versions 3.6 to 3.6.1, 3.5 to 3.5.3, 3.4 to 3.4.6, 3.1 to 3.1.15 and earlier unsupported versions. The 'manage groups' capability did not have the 'XSS risk' flag assigned to it, but does have that access in certain places. Note that the capability is intended for use by trusted users, and is only assigned to teachers and managers by default. **CVE ID : CVE-2019-3808**	https://moodle.org/mod/forum/discuss.php?d=381228#p1536765	A-MOO-MOOD-040419/268
N/A	25-03-2019	7.5	A flaw was found in Moodle versions 3.1 to 3.1.15 and earlier unsupported versions. The mybackpack functionality allowed setting the URL of badges, when it should be restricted to the Mozilla Open Badges backpack URL. This resulted in the possibility of blind SSRF via requests made by the page. **CVE ID : CVE-2019-3809**	https://moodle.org/mod/forum/discuss.php?d=381229#p1536766	A-MOO-MOOD-040419/269
N/A	25-03-2019	5	A flaw was found in	https://moo	A-MOO-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			moodle versions 3.6 to 3.6.1, 3.5 to 3.5.3, 3.4 to 3.4.6, 3.1 to 3.1.15 and earlier unsupported versions. The /userpix/ page did not escape users' full names, which are included as text when hovering over profile images. Note this page is not linked to by default and its access is restricted. **CVE ID : CVE-2019-3810**	dle.org/mod/forum/discuss.php?d=381230#p1536767	MOOD-040419/270
N/A	27-03-2019	6.5	A vulnerability was found in moodle before versions 3.6.3, 3.5.5, 3.4.8 and 3.1.17. Users with the "login as other users" capability (such as administrators/managers) can access other users' Dashboards, but the JavaScript those other users may have added to their Dashboard was not being escaped when being viewed by the user logging in on their behalf. **CVE ID : CVE-2019-3847**	N/A	A-MOO-MOOD-040419/271
N/A	26-03-2019	4	A vulnerability was found in moodle before versions 3.6.3, 3.5.5 and 3.4.8. Permissions were not correctly checked before loading event information into the calendar's edit event modal popup, so	N/A	A-MOO-MOOD-040419/272

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			logged in non-guest users could view unauthorised calendar events. (Note: It was read-only access, users could not edit the events.) **CVE ID : CVE-2019-3848**		
N/A	26-03-2019	6.5	A vulnerability was found in moodle before versions 3.6.3, 3.5.5 and 3.4.8. Users could assign themselves an escalated role within courses or content accessed via LTI, by modifying the request to the LTI publisher site. **CVE ID : CVE-2019-3849**	N/A	A-MOO-MOOD-040419/273
N/A	26-03-2019	5.8	A vulnerability was found in moodle before versions 3.6.3, 3.5.5, 3.4.8 and 3.1.17. Links within assignment submission comments would open directly (in the same window). Although links themselves may be valid, opening within the same window and without the no-referrer header policy made them more susceptible to exploits. **CVE ID : CVE-2019-3850**	N/A	A-MOO-MOOD-040419/274
N/A	26-03-2019	4	A vulnerability was found in moodle before versions 3.6.3 and 3.5.5. There was a link to site home within the the Boost theme's	N/A	A-MOO-MOOD-040419/275

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			secure layout, meaning students could navigate out of the page. **CVE ID : CVE-2019-3851**		
N/A	26-03-2019	4	A vulnerability was found in moodle before version 3.6.3. The get_with_capability_join and get_users_by_capability functions were not taking context freezing into account when checking user capabilities **CVE ID : CVE-2019-3852**	N/A	A-MOO-MOOD-040419/276
morgan_project					
morgan					
N/A	21-03-2019	7.5	An attacker can use the format parameter to inject arbitrary commands in the npm package morgan < 1.9.1. **CVE ID : CVE-2019-5413**	N/A	A-MOR-MORG-040419/277
Moxa					
Softcms					
N/A	21-03-2019	6.8	Moxa SoftCMS 1.3 and prior is susceptible to a buffer overflow condition that may crash or allow remote code execution. Moxa released SoftCMS version 1.4 on June 1, 2015, to address the vulnerability. **CVE ID : CVE-2015-6457**	N/A	A-MOX-SOFT-040419/278

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	6.8	Moxa SoftCMS 1.3 and prior is susceptible to a buffer overflow condition that may crash or allow remote code execution. Moxa released SoftCMS version 1.4 on June 1, 2015, to address the vulnerability. **CVE ID : CVE-2015-6458**	N/A	A-MOX-SOFT-040419/279
myadrenalin					
adrenalin					
N/A	25-03-2019	4.3	A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in Adrenalin 5.4 HRMS Software. The user supplied input containing JavaScript is echoed back in JavaScript code in an HTML response via the LeaveEmployeeSearch.aspx prntFrmName or prntDDLCntrlName parameter. **CVE ID : CVE-2018-12652**	N/A	A-MYA-ADRE-040419/280
N/A	25-03-2019	4.3	A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in Adrenalin 5.4 HRMS Software. The user supplied input containing JavaScript is echoed back in JavaScript code in an HTML response via the	N/A	A-MYA-ADRE-040419/281

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RPT/SSRSDynamicEditReports.aspx ReportId parameter. **CVE ID : CVE-2018-12653**		
Mybb					
Mybb					
N/A	29-03-2019	4.3	A reflected XSS vulnerability in the ModCP Profile Editor in MyBB before 1.8.20 allows remote attackers to inject JavaScript via the 'username' parameter. **CVE ID : CVE-2018-19201**	N/A	A-MYB-MYBB-040419/282
trash_bin					
N/A	21-03-2019	6.8	Trash Bin plugin 1.1.3 for MyBB has cross-site scripting (XSS) via a thread subject and a cross-site request forgery (CSRF) via a post subject. **CVE ID : CVE-2018-14575**	N/A	A-MYB-TRAS-040419/283
ban_list					
N/A	21-03-2019	3.5	In the Ban List plugin 1.0 for MyBB, any forum user with mod privileges can ban users and input an XSS payload into the ban reason, which is executed on the bans.php page. **CVE ID : CVE-2018-14724**	N/A	A-MYB-BAN_-040419/284
Nagios					
nagios_xi					
N/A	28-03-2019	6.5	Command injection in	https://ww	A-NAG-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nagios XI before 5.5.11 allows an authenticated users to execute arbitrary remote commands via a new autodiscovery job. **CVE ID : CVE-2019-9164**	w.nagios.com/products/security/	NAGI-040419/285
N/A	28-03-2019	7.5	SQL injection vulnerability in Nagios XI before 5.5.11 allows attackers to execute arbitrary SQL commands via the API when using fusekeys and malicious user id. **CVE ID : CVE-2019-9165**	https://www.nagios.com/products/security/	A-NAG-NAGI-040419/286
N/A	28-03-2019	7.2	Privilege escalation in Nagios XI before 5.5.11 allows local attackers to elevate privileges to root via write access to config.inc.php and import_xiconfig.php. **CVE ID : CVE-2019-9166**	https://www.nagios.com/products/security/	A-NAG-NAGI-040419/287
N/A	28-03-2019	4.3	Cross-site scripting (XSS) vulnerability in Nagios XI before 5.5.11 allows attackers to inject arbitrary web script or HTML via the xiwindow parameter. **CVE ID : CVE-2019-9167**	https://www.nagios.com/products/security/	A-NAG-NAGI-040419/288
Netapp					
ontap_select_deploy_administration_utility					
N/A	21-03-2019	9.3	An integer overflow flaw which could lead to an out of bounds write was	N/A	A-NET-ONTA-040419/289

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3855**		
N/A	25-03-2019	6.8	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server. **CVE ID : CVE-2019-3856**	N/A	A-NET-ONTA-040419/290
N/A	25-03-2019	6.8	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.	N/A	A-NET-ONTA-040419/291

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3857		
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3858**	N/A	A-NET-ONTA-040419/292
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3859**	N/A	A-NET-ONTA-040419/293
N/A	25-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	N/A	A-NET-ONTA-040419/294

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3860		
N/A	25-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3861**	N/A	A-NET-ONTA-040419/295
N/A	21-03-2019	6.4	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE ID : CVE-2019-3862**	N/A	A-NET-ONTA-040419/296
N/A	25-03-2019	6.8	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy	N/A	A-NET-ONTA-040419/297

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory causing in an out of bounds memory write error. **CVE ID : CVE-2019-3863**		
Nodejs					
Node.js					
N/A	28-03-2019	5	Keep-alive HTTP and HTTPS connections can remain open and inactive for up to 2 minutes in Node.js 6.16.0 and earlier. Node.js 8.0.0 introduced a dedicated server.keepAliveTimeout which defaults to 5 seconds. The behavior in Node.js 6.16.0 and earlier is a potential Denial of Service (DoS) attack vector. Node.js 6.17.0 introduces server.keepAliveTimeout and the 5-second default. **CVE ID : CVE-2019-5739**	N/A	A-NOD-NODE-040419/298
node-opencv_project					
node-opencv					
N/A	25-03-2019	7.5	utils/find-opencv.js in node-opencv (aka OpenCV bindings for Node.js) prior to 6.1.0 is vulnerable to Command Injection. It does not validate user input allowing attackers to execute arbitrary commands.	N/A	A-NOD-NODE-040419/299

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10061		
Omron					
poweract_pro_master_agent					
N/A	27-03-2019	4	PowerAct Pro Master Agent for Windows Version 5.13 and earlier allows authenticated attackers to bypass access restriction to alter or edit unauthorized files via unspecified vectors. **CVE ID : CVE-2018-16207**	N/A	A-OMR-POWE-040419/300
online_lottery_php_readymade_script_project					
online_lottery_php_readymade_script					
N/A	29-03-2019	6.8	PHP Scripts Mall Online Lottery PHP Readymade Script 1.7.0 has Cross-Site Request Forgery (CSRF) for Edit Profile actions. **CVE ID : CVE-2019-9604**	N/A	A-ONL-ONLI-040419/301
N/A	29-03-2019	3.5	PHP Scripts Mall Online Lottery PHP Readymade Script 1.7.0 has Reflected Cross-site Scripting (XSS) via the err value in a .ico picture upload. **CVE ID : CVE-2019-9605**	N/A	A-ONL-ONLI-040419/302
openmicroscopy					
omero					
N/A	31-03-2019	6.8	OMERO before 5.0.6 has multiple CSRF vulnerabilities because the framework for OMERO's web interface lacks CSRF	N/A	A-OPE-OMER-040419/303

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protection. **CVE ID : CVE-2014-7198**		
opensource_classified_ads_script_project					
opensource_classified_ads_script					
N/A	21-03-2019	5	PHP Scripts Mall Opensource Classified Ads Script 3.2.2 has reflected HTML injection via the Search Form. **CVE ID : CVE-2019-7435**	N/A	A-OPE-OPEN-040419/304
N/A	21-03-2019	4	PHP Scripts Mall Opensource Classified Ads Script 3.2.2 has directory traversal via a direct request for a listing of an uploads directory. **CVE ID : CVE-2019-7436**	N/A	A-OPE-OPEN-040419/305
N/A	21-03-2019	4.3	PHP Scripts Mall Opensource Classified Ads Script 3.2.2 has reflected Cross-Site Scripting (XSS) via the Search field. **CVE ID : CVE-2019-7437**	N/A	A-OPE-OPEN-040419/306
Openstack					
Ceilometer					
N/A	26-03-2019	4	A vulnerability was found in ceilometer before version 12.0.0.0rc1. An Information Exposure in ceilometer-agent prints sensitive configuration data to log files without DEBUG logging being activated.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3830	A-OPE-CEIL-040419/307

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3830		
Opentext					
opentext_portal					
N/A	22-03-2019	4.3	Cross-site scripting (XSS) vulnerability in OpenText Portal 7.4.4 allows remote attackers to inject arbitrary web script or HTML via the vgnextoid parameter to a menuitem URI. **CVE ID : CVE-2018-20165**	N/A	A-OPE-OPEN-040419/308
Open-xchange					
open-xchange_appsuite					
N/A	21-03-2019	5.5	OX App Suite 7.8.4 and earlier allows SSRF. **CVE ID : CVE-2018-13103**	N/A	A-OPE-OPEN-040419/309
N/A	21-03-2019	3.5	OX App Suite 7.8.4 and earlier allows XSS. Internal reference: 58742 (Bug ID) **CVE ID : CVE-2018-13104**	N/A	A-OPE-OPEN-040419/310
Opera					
opera_browser					
N/A	21-03-2019	9.3	Opera before 57.0.3098.106 is vulnerable to a DLL Search Order hijacking attack where an attacker can send a ZIP archive composed of an HTML page along with a malicious DLL to the target. Once the document is opened, it may allow the	N/A	A-OPE-OPER-040419/311

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to take full control of the system from any location within the system. The issue lies in the loading of the shcore.dll and dcomp.dll files: these files are being searched for by the program in the same system-wide directory where the HTML file is executed. **CVE ID : CVE-2018-18913**		
Ovirt					
vdsm					
N/A	25-03-2019	9	A vulnerability was discovered in vdsm, version 4.19 through 4.30.3 and 4.30.5 through 4.30.8. The systemd_run function exposed to the vdsm system user could be abused to execute arbitrary commands as root. **CVE ID : CVE-2019-3831**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3831	A-OVI-VDSM-040419/312
Ovirt					
N/A	25-03-2019	4	In ovirt-engine 4.1, if a host was provisioned with cloud-init, the root password could be revealed through the REST interface. **CVE ID : CVE-2017-7510**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-7510	A-OVI-OVIR-040419/313
N/A	25-03-2019	5.5	It was discovered that in the ovirt's REST API before version 4.3.2.1,	https://bugzilla.redhat.com/show_bug	A-OVI-OVIR-040419/314

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RemoveDiskCommand is triggered as an internal command, meaning the permission validation that should be performed against the calling user is skipped. A user with low privileges (eg Basic Operations) could exploit this flaw to delete disks attached to guests. **CVE ID : CVE-2019-3879**	.cgi?id=CVE-2019-3879	
Paloaltonetworks					
Expedition					
N/A	26-03-2019	3.5	The Expedition Migration tool 1.1.8 and earlier may allow an authenticated attacker to run arbitrary JavaScript or HTML in the User Mapping Settings for account name of admin user. **CVE ID : CVE-2019-1569**	N/A	A-PAL-EXPE-040419/315
N/A	26-03-2019	3.5	The Expedition Migration tool 1.1.8 and earlier may allow an authenticated attacker to run arbitrary JavaScript or HTML in the LDAP server settings. **CVE ID : CVE-2019-1570**	N/A	A-PAL-EXPE-040419/316
N/A	26-03-2019	3.5	The Expedition Migration tool 1.1.8 and earlier may allow an authenticated attacker to run arbitrary JavaScript or HTML in the RADIUS server settings.	N/A	A-PAL-EXPE-040419/317

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1571		
pdfalto_project					
pdfalto					
N/A	21-03-2019	6.8	There is an invalid memory access in the function GfxIndexedColorSpace::mapColorToBase() located in GfxState.cc in Xpdf 4.0.0, as used in pdfalto 0.2. It can be triggered by (for example) sending a crafted pdf file to the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2019-9878**	N/A	A-PDF-PDFA-040419/318
Phpcms					
Phpcms					
N/A	24-03-2019	3.5	PHPCMS 9.6.x through 9.6.3 has XSS via the mailbox (aka E-mail) field on the personal information screen. **CVE ID : CVE-2019-10027**	N/A	A-PHP-PHPC-040419/319
portainer					
portainer					
N/A	27-03-2019	5	A vulnerability was found in Portainer before 1.20.0. Portainer stores LDAP credentials, corresponding to a master password, in cleartext and allows their	N/A	A-POR-PORT-040419/320

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			retrieval via API calls. **CVE ID : CVE-2018-19466**		
Powerdns					
authoritative_server					
N/A	21-03-2019	6.5	A vulnerability was found in PowerDNS Authoritative Server before 4.0.7 and before 4.1.7. An insufficient validation of data coming from the user when building a HTTP request from a DNS query in the HTTP Connector of the Remote backend, allowing a remote user to cause a denial of service by making the server connect to an invalid endpoint, or possibly information disclosure by making the server connect to an internal endpoint and somehow extracting meaningful information about the response **CVE ID : CVE-2019-3871**	N/A	A-POW-AUTH-040419/321
printeron					
printeron					
N/A	21-03-2019	3.5	PrinterOn Enterprise 4.1.4 suffers from multiple authenticated stored XSS vulnerabilities via the (1) "Machine Host Name" or "Server Serial Number" field in the clustering	N/A	A-PRI-PRIN-040419/322

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration, (2) "name" field in the Edit Group configuration, (3) "Rule Name" field in the Access Control configuration, (4) "Service Name" in the Service Configuration, or (5) First Name or Last Name field in the Edit Account configuration. **CVE ID : CVE-2018-17167**		
Puppet					
chloride					
N/A	21-03-2019	5	Prior to version 0.3.0, chloride's use of net-ssh resulted in host fingerprints for previously unknown hosts getting added to the user's known_hosts file without confirmation. In version 0.3.0 this is updated so that the user's known_hosts file is not updated by chloride. **CVE ID : CVE-2018-6517**	https://puppet.com/security/cve/CVE-2018-6517	A-PUP-CHLO-040419/323
Python					
Python					
N/A	23-03-2019	4.3	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the	N/A	A-PYT-PYTH-040419/324

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			first argument to urllib.request.urlopen with \r\n (specifically in the query string or PATH_INFO) followed by an HTTP header or a Redis command. This is similar to CVE-2019-9740. **CVE ID : CVE-2019-9947**		
N/A	23-03-2019	6.4	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call. **CVE ID : CVE-2019-9948**	N/A	A-PYT-PYTH-040419/325
pytroll					
donfig					
N/A	21-03-2019	7.5	An issue was discovered in Donfig 0.3.0. There is a vulnerability in the collect_yaml method in config_obj.py. It can execute arbitrary Python commands, resulting in command execution. **CVE ID : CVE-2019-7537**	N/A	A-PYT-DONF-040419/326
Qemu					
Qemu					
N/A	21-03-2019	2.1	In QEMU 3.1,	N/A	A-QEM-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scsi_handle_inquiry_reply in hw/scsi/scsi-generic.c allows out-of-bounds write and read operations. **CVE ID : CVE-2019-6501**		QEMU-040419/327
N/A	21-03-2019	2.1	hw/ppc/spapr.c in QEMU through 3.1.0 allows Information Exposure because the hypervisor shares the /proc/device-tree/system-id and /proc/device-tree/model system attributes with a guest. **CVE ID : CVE-2019-8934**	N/A	A-QEM-QEMU-040419/328
QT					
QT					
N/A	21-03-2019	4.3	An issue was discovered in Qt 5.11. A malformed PPM image causes a division by zero and a crash in qppmhandler.cpp. **CVE ID : CVE-2018-19872**	N/A	A-QT-QT-040419/329
Redhat					
Libvirt					
N/A	27-03-2019	3.5	A NULL pointer dereference flaw was discovered in libvirt before version 5.0.0 in the way it gets interface information through the QEMU agent. An attacker in a guest VM can use this flaw to crash libvirtd and cause a denial of service.	https://www.redhat.com/archives/libvir-list/2019-January/msg00241.html	A-RED-LIBV-040419/330

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3840		
ansible					
N/A	27-03-2019	7.5	Ansible fetch module before versions 2.5.15, 2.6.14, 2.7.8 has a path traversal vulnerability which allows copying and overwriting files outside of the specified destination in the local ansible controller host, by not restricting an absolute path. **CVE ID : CVE-2019-3828**	N/A	A-RED-ANSI-040419/331
gluster_storage					
N/A	25-03-2019	9	A vulnerability was discovered in vdsm, version 4.19 through 4.30.3 and 4.30.5 through 4.30.8. The systemd_run function exposed to the vdsm system user could be abused to execute arbitrary commands as root. **CVE ID : CVE-2019-3831**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3831	A-RED-GLUS-040419/332
ansible_tower					
N/A	28-03-2019	4	When running Tower before 3.4.3 on OpenShift or Kubernetes, application credentials are exposed to playbook job runs via environment variables. A malicious user with the ability to write playbooks could use this to gain administrative privileges.	N/A	A-RED-ANSI-040419/333

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3869		
Openstack					
N/A	26-03-2019	4	A vulnerability was found in ceilometer before version 12.0.0.0rc1. An Information Exposure in ceilometer-agent prints sensitive configuration data to log files without DEBUG logging being activated. **CVE ID : CVE-2019-3830**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3830	A-RED-OPEN-040419/334
risi					
gestao_de_horarios					
N/A	21-03-2019	6.5	RISI Gestao de Horarios v3201.09.08 rev.23 allows SQL Injection. **CVE ID : CVE-2019-6491**	N/A	A-RIS-GEST-040419/335
robocode_project					
robocode					
N/A	30-03-2019	7.5	Robocode through 1.9.3.5 allows remote attackers to cause external service interaction (DNS), as demonstrated by a query for a unique subdomain name within an attacker-controlled DNS zone, because of a .openStream call within java.net.URL. **CVE ID : CVE-2019-10648**	N/A	A-ROB-ROBO-040419/336
Rockwellautomation					
Ethernet/ip_web_server_module_1756-eweb					
N/A	27-03-2019	7.8	Rockwell Automation	N/A	A-ROC-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EtherNet/IP Web Server Modules 1756-EWEB (includes 1756-EWEBK) Version 5.001 and earlier, and CompactLogix 1768-EWEB Version 2.005 and earlier. A remote attacker could send a crafted UDP packet to the SNMP service causing a denial-of-service condition to occur until the affected product is restarted. **CVE ID : CVE-2018-19016**		ETHE-040419/337
Ethernet/ip_web_server_module_1768-eweb					
N/A	27-03-2019	7.8	Rockwell Automation EtherNet/IP Web Server Modules 1756-EWEB (includes 1756-EWEBK) Version 5.001 and earlier, and CompactLogix 1768-EWEB Version 2.005 and earlier. A remote attacker could send a crafted UDP packet to the SNMP service causing a denial-of-service condition to occur until the affected product is restarted. **CVE ID : CVE-2018-19016**	N/A	A-ROC-ETHE-040419/338
Samsung					
syncthru_web_service					
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015	N/A	A-SAM-SYNC-040419/339

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in "/sws/swsAlert.sws" in multiple parameters: flag, frame, func, and Nfunc. **CVE ID : CVE-2019-7418**		
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in "/sws/leftmenu.sws" in multiple parameters: ruiFw_id, ruiFw_pid, ruiFw_title. **CVE ID : CVE-2019-7419**	N/A	A-SAM-SYNC-040419/340
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in "/sws.application/information/networkinformationView.sws" in the tabName parameter. **CVE ID : CVE-2019-7420**	N/A	A-SAM-SYNC-040419/341
N/A	21-03-2019	4.3	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in "/sws.login/gnb/loginView.sws" in multiple parameters: contextpath and basedURL. **CVE ID : CVE-2019-7421**	N/A	A-SAM-SYNC-040419/342
S-cms					
S-cms					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-03-2019	6.8	S-CMS PHP v1.0 has a CSRF vulnerability to add a new admin user via the 4.edu.php/admin/ajax.php ?type=admin&action=add &lang=0 URI, a related issue to CVE-2019-9040. **CVE ID : CVE-2019-10237**	N/A	A-S-C-S-CM-040419/343
select2					
select2					
N/A	27-03-2019	4.3	In Select2 through 4.0.5, as used in Snipe-IT and other products, rich selectlists allow XSS. This affects use cases with Ajax remote data loading when HTML templates are used to display listbox data. **CVE ID : CVE-2016-10744**	N/A	A-SEL-SELE-040419/344
shellinabox_project					
shellinabox					
N/A	21-03-2019	7.8	libhttp/url.c in shellinabox through 2.20 has an implementation flaw in the HTTP request parsing logic. By sending a crafted multipart/form-data HTTP request, an attacker could exploit this to force shellinaboxd into an infinite loop, exhausting available CPU resources and taking the service down. **CVE ID : CVE-2018-16789**	https://github.com/shellinabox/shellinabox/commit/4f0ecc31ac6f985e0dd3f5a52cbfc0e9251f6361	A-SHE-SHEL-040419/345

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sitemagic					
sitemagic					
N/A	27-03-2019	4.3	Sitemagic CMS v4.4 has XSS in SMFiles/FrmUpload.class.php via the filename parameter. **CVE ID : CVE-2019-10238**	N/A	A-SIT-SITE-040419/346
softnas					
cloud					
N/A	23-03-2019	10	SoftNAS Cloud 4.2.0 and 4.2.1 allows remote command execution. The NGINX default configuration file has a check to verify the status of a user cookie. If not set, a user is redirected to the login page. An arbitrary value can be provided for this cookie to access the web interface without valid user credentials. If customers have not followed SoftNAS deployment best practices and expose SoftNAS StorageCenter ports directly to the internet, this vulnerability allows an attacker to gain access to the Webadmin interface to create new users or execute arbitrary commands with administrative privileges, compromising both the	N/A	A-SOF-CLOU-040419/347

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			platform and the data. **CVE ID : CVE-2019-9945**		
Solarwinds					
serv-u_ftp_server					
N/A	21-03-2019	3.5	SolarWinds Serv-U FTP Server 15.1.6.25 has reflected cross-site scripting (XSS) in the Web management interface via URL path and HTTP POST parameter. **CVE ID : CVE-2018-19934**	N/A	A-SOL-SERV-040419/348
Sonatype					
Nexus					
N/A	21-03-2019	7.5	Sonatype Nexus Repository Manager before 3.15.0 has Incorrect Access Control. **CVE ID : CVE-2019-7238**	N/A	A-SON-NEXU-040419/349
Sqlite					
Sqlite					
N/A	22-03-2019	5	In SQLite 3.27.2, running fts5 prefix queries inside a transaction could trigger a heap-based buffer over-read in fts5HashEntrySort in sqlite3.c, which may lead to an information leak. This is related to ext/fts5/fts5_hash.c. **CVE ID : CVE-2019-9936**	N/A	A-SQL-SQLI-040419/350
N/A	22-03-2019	5	In SQLite 3.27.2, interleaving reads and writes in a single	N/A	A-SQL-SQLI-040419/351

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			transaction with an fts5 virtual table will lead to a NULL Pointer Dereference in fts5ChunkIterate in sqlite3.c. This is related to ext/fts5/fts5_hash.c and ext/fts5/fts5_index.c. **CVE ID : CVE-2019-9937**		
Sqlitemanager					
Sqlitemanager					
N/A	21-03-2019	7.5	SQLiteManager 1.20 and 1.24 allows SQL injection via the /sqlitemanager/main.php dbsel parameter. NOTE: This product is discontinued. **CVE ID : CVE-2019-9083**	N/A	A-SQL-SQLI-040419/352
sricam					
gsoap					
N/A	21-03-2019	5	Sricam IP CCTV cameras are vulnerable to denial of service via multiple incomplete HTTP requests because the web server (based on gSOAP 2.8.x) is configured for an iterative queueing approach (aka non-threaded operation) with a timeout of several seconds. **CVE ID : CVE-2019-6973**	N/A	A-SRI-GSOA-040419/353
symfony					
twig					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	23-03-2019	4.3	A sandbox information disclosure exists in Twig before 1.38.0 and 2.x before 2.7.0 because, under some circumstances, it is possible to call the __toString() method on an object even if not allowed by the security policy in place. **CVE ID : CVE-2019-9942**	N/A	A-SYM-TWIG-040419/354
teclib-edition					
gestionnaire_libre_de_parc_informatique					
N/A	27-03-2019	7.5	Teclib GLPI through 9.3.3 has SQL injection via the "cycle" parameter in /scripts/unlock_tasks.php. **CVE ID : CVE-2019-10232**	N/A	A-TEC-GEST-040419/355
thereceptionist					
the_receptionist_for_ipad					
N/A	21-03-2019	2.1	The Receptionist for iPad could allow a local attacker to obtain sensitive information, caused by an error in the contact.json file. An attacker could exploit this vulnerability to obtain the contact names, phone numbers and emails. **CVE ID : CVE-2018-17502**	N/A	A-THE-THE_-040419/356
tianocore					
edk_ii					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-03-2019	6.4	Buffer overflow in network stack for EDK II may allow unprivileged user to potentially enable escalation of privilege and/or denial of service via network. **CVE ID : CVE-2018-12178**	https://edk2-docs.gitbooks.io/security-advisory/content/dns-pack-size-check.html	A-TIA-EDK_-040419/357
N/A	27-03-2019	4.6	Improper configuration in system firmware for EDK II may allow unauthenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access. **CVE ID : CVE-2018-12179**	https://edk2-docs.gitbooks.io/security-advisory/content/opal-blocksid-setting-disabled-after-s3.html	A-TIA-EDK_-040419/358
N/A	27-03-2019	6.8	Buffer overflow in BlockIo service for EDK II may allow an unauthenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via network access. **CVE ID : CVE-2018-12180**	https://edk2-docs.gitbooks.io/security-advisory/content/buffer-overflow-in-blockio-service-for-ram-disk.html	A-TIA-EDK_-040419/359
N/A	27-03-2019	3.6	Stack overflow in corrupted bmp for EDK II may allow unprivileged user to potentially enable denial of service or elevation of privilege via local access.	https://edk2-docs.gitbooks.io/security-advisory/content/stack-overflow-on-corrupted-	A-TIA-EDK_-040419/360

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-12181	bmp.html	
N/A	27-03-2019	4.6	Insufficient memory write check in SMM service for EDK II may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access. **CVE ID : CVE-2018-12182**	https://edk2-docs.gitbooks.io/security-advisory/content/sw-smi-confused-deputy-smramsavestate_c.html	A-TIA-EDK_-040419/361
N/A	27-03-2019	4.6	Stack overflow in DxeCore for EDK II may allow an unauthenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access. **CVE ID : CVE-2018-12183**	https://edk2-docs.gitbooks.io/security-advisory/content/unlimited-fv-recursion.html	A-TIA-EDK_-040419/362
N/A	27-03-2019	4.6	Logic issue in variable service module for EDK II/UDK2018/UDK2017/UDK2015 may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access. **CVE ID : CVE-2018-3613**	https://edk2-docs.gitbooks.io/security-advisory/content/authvariable-timestamp-zeroing-on-append_write.html	A-TIA-EDK_-040419/363
N/A	27-03-2019	7.5	Buffer overflow in system firmware for EDK II may allow unauthenticated user to potentially enable escalation of privilege	https://edk2-docs.gitbooks.io/security-advisory/con	A-TIA-EDK_-040419/364

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and/or denial of service via network access. **CVE ID : CVE-2019-0160**	tent/partitiondxe-and-udf-buffer-overflow.html	
N/A	27-03-2019	2.1	Stack overflow in XHCI for EDK II may allow an unauthenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0161**	https://edk2-docs.gitbooks.io/security-advisory/content/xhci-stack-local-stack-overflow.html	A-TIA-EDK_-040419/365
Tibco					
data_science_for_aws					
N/A	26-03-2019	3.5	The application server component of TIBCO Software Inc.'s TIBCO Data Science for AWS, and TIBCO Spotfire Data Science contains a persistent cross-site scripting vulnerability that theoretically allows an authenticated user to gain access to all the capabilities of the web interface available to more privileged users. Affected releases are TIBCO Software Inc.'s TIBCO Data Science for AWS: versions up to and including 6.4.0, and TIBCO Spotfire Data Science: versions up to and	N/A	A-TIB-DATA-040419/366

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including 6.4.0. **CVE ID : CVE-2019-8987**		
N/A	26-03-2019	5.5	The application server component of TIBCO Software Inc.'s TIBCO Data Science for AWS, and TIBCO Spotfire Data Science contains a persistent cross-site contains a vulnerability that theoretically allows a user to escalate their privileges on the affected system, in a way that may allow for data modifications and deletions that should be denied. Affected releases are TIBCO Software Inc.'s TIBCO Data Science for AWS: versions up to and including 6.4.0, and TIBCO Spotfire Data Science: versions up to and including 6.4.0. **CVE ID : CVE-2019-8988**	N/A	A-TIB-DATA-040419/367
N/A	26-03-2019	4	The application server component of TIBCO Software Inc.'s TIBCO Data Science for AWS, and TIBCO Spotfire Data Science contains a vulnerability that theoretically enables a user to spoof their account to look like a different user in the affected system.	N/A	A-TIB-DATA-040419/368

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Affected releases are TIBCO Software Inc.'s TIBCO Data Science for AWS: versions up to and including 6.4.0, and TIBCO Spotfire Data Science: versions up to and including 6.4.0. **CVE ID : CVE-2019-8989**		
spotfire_data_science					
N/A	26-03-2019	3.5	The application server component of TIBCO Software Inc.'s TIBCO Data Science for AWS, and TIBCO Spotfire Data Science contains a persistent cross-site scripting vulnerability that theoretically allows an authenticated user to gain access to all the capabilities of the web interface available to more privileged users. Affected releases are TIBCO Software Inc.'s TIBCO Data Science for AWS: versions up to and including 6.4.0, and TIBCO Spotfire Data Science: versions up to and including 6.4.0. **CVE ID : CVE-2019-8987**	N/A	A-TIB-SPOT-040419/369
N/A	26-03-2019	5.5	The application server component of TIBCO Software Inc.'s TIBCO Data Science for AWS, and TIBCO Spotfire Data	N/A	A-TIB-SPOT-040419/370

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Science contains a persistent cross-site contains a vulnerability that theoretically allows a user to escalate their privileges on the affected system, in a way that may allow for data modifications and deletions that should be denied. Affected releases are TIBCO Software Inc.'s TIBCO Data Science for AWS: versions up to and including 6.4.0, and TIBCO Spotfire Data Science: versions up to and including 6.4.0. **CVE ID : CVE-2019-8988**		
N/A	26-03-2019	4	The application server component of TIBCO Software Inc.'s TIBCO Data Science for AWS, and TIBCO Spotfire Data Science contains a vulnerability that theoretically enables a user to spoof their account to look like a different user in the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Data Science for AWS: versions up to and including 6.4.0, and TIBCO Spotfire Data Science: versions up to and including 6.4.0.	N/A	A-TIB-SPOT-040419/371

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8989		
totaljs					
total.js_cms					
N/A	28-03-2019	4.3	Total.js CMS 12.0.0 has XSS related to themes/admin/views/index.html (item.message) and themes/admin/public/ui.js (column.format). **CVE ID : CVE-2019-10260**	N/A	A-TOT-TOTA-040419/372
trustsource					
ecs_publisher					
N/A	28-03-2019	4	A vulnerability in Jenkins ECS Publisher Plugin 1.0.0 and earlier allows attackers with Item/Extended Read permission, or local file system access to the Jenkins home directory to obtain the API token configured in this plugin's configuration. **CVE ID : CVE-2019-1003045**	N/A	A-TRU-ECS_-040419/373
Ucweb					
uc_browser					
N/A	28-03-2019	4.3	UCWeb UC Browser 7.0.185.1002 on Windows uses HTTP for downloading certain PDF modules, which allows MITM attacks.	N/A	A-UCW-UC_B-040419/374

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10250		
ushareit					
shareit					
N/A	22-03-2019	5.8	The SHAREit application before 4.0.36 for Android allows a remote attacker (on the same network or joining public "open" Wi-Fi hotspots created by the application when file transfer is initiated) to bypass authentication by trying to fetch a non-existing page. When the non-existing page is requested, the application responds with a 200 status code and empty page, and adds the requesting client device into the list of recognized devices. **CVE ID : CVE-2019-9939**	N/A	A-USH-SHAR-040419/375
Verifone					
verix_multi-app_conductor					
N/A	25-03-2019	6.8	The Verix Multi-app Conductor application 2.7 for Verifone Verix suffers from a buffer overflow vulnerability that allows attackers to execute arbitrary code via a long configuration key value. An attacker must be able to download files to the device in order to exploit this vulnerability.	N/A	A-VER-VERI-040419/376

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10060		
Veritas					
netbackup_appliance					
N/A	21-03-2019	4	An issue was discovered in the Web Console in Veritas NetBackup Appliance through 3.1.2. The proxy server password is displayed to an administrator. **CVE ID : CVE-2019-9867**	N/A	A-VER-NETB-040419/377
N/A	21-03-2019	4	An issue was discovered in the Web Console in Veritas NetBackup Appliance through 3.1.2. The SMTP password is displayed to an administrator. **CVE ID : CVE-2019-9868**	N/A	A-VER-NETB-040419/378
vertrigoserv_project					
vertrigoserv					
N/A	21-03-2019	4.3	VertrigoServ 2.17 allows XSS via the /inc/extensions.php ext parameter. **CVE ID : CVE-2019-8938**	N/A	A-VER-VERT-040419/379
W1.fi					
Hostapd					
N/A	23-03-2019	5	hostapd before 2.6 does not prevent use of the low-quality PRNG that is reached by an os_random() function call. **CVE ID : CVE-2016-10743**	N/A	A-W1.-HOST-040419/380

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
weban					
an					
N/A	27-03-2019	5	Directory traversal vulnerability in 'an' App for iOS Version 3.2.0 and earlier allows remote attackers to read arbitrary files via unspecified vectors. **CVE ID : CVE-2019-5927**	N/A	A-WEB-AN-040419/381
website_seller_script_project					
website_seller_script					
N/A	21-03-2019	5	PHP Scripts Mall Website Seller Script 2.0.5 allows full Path Disclosure via a request for an arbitrary image URL such as a .png file. **CVE ID : CVE-2018-20631**	N/A	A-WEB-WEBS-040419/382
We-con					
pi_studio					
N/A	27-03-2019	4.3	WECON Technology PI Studio HMI versions 4.1.9 and prior and PI Studio versions 4.2.34 and prior lacks proper validation of user-supplied data, which may result in a read past the end of an allocated object. **CVE ID : CVE-2018-14814**	N/A	A-WE--PI_S-040419/383
pi_studio_hmi					
N/A	27-03-2019	4.3	WECON Technology PI Studio HMI versions 4.1.9	N/A	A-WE--PI_S-040419/384

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior and PI Studio versions 4.2.34 and prior lacks proper validation of user-supplied data, which may result in a read past the end of an allocated object. **CVE ID : CVE-2018-14814**		
Wolfcms					
wolfcms					
N/A	29-03-2019	4.3	Wolf CMS v0.8.3.1 is affected by cross site scripting (XSS) in the module Add Snippet (/?/admin/snippet/add). This allows an attacker to insert arbitrary JavaScript as user input, which will be executed whenever the affected snippet is loaded. **CVE ID : CVE-2019-10646**	N/A	A-WOL-WOLF-040419/385
Woocommerce					
paypal_checkout_payment_gateway					
N/A	21-03-2019	4	cgi-bin/webscr?cmd=_cart in the WooCommerce PayPal Checkout Payment Gateway plugin 1.6.8 for WordPress allows Parameter Tampering in an amount parameter (such as amount_1), as demonstrated by purchasing an item for lower than the intended price.	N/A	A-WOO-PAYP-040419/386

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7441		
wpsupportplus					
wp_support_plus_responsive_ticket_system					
N/A	21-03-2019	4.3	A stored cross-site scripting (XSS) vulnerability in the submit_ticket.php module in the WP Support Plus Responsive Ticket System plugin 9.1.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the subject parameter in wp-content/plugins/wp-support-plus-responsive-ticket-system/includes/ajax/submit_ticket.php. **CVE ID : CVE-2019-7299**	N/A	A-WPS-WP_S-040419/387
Wso2					
api_manager					
N/A	21-03-2019	3.5	An issue was discovered in WSO2 API Manager 2.1.0 and 2.6.0. A DOM-based XSS exists in the store part of the product. **CVE ID : CVE-2018-20736**	N/A	A-WSO-API_-040419/388
N/A	21-03-2019	3.5	An issue was discovered in WSO2 API Manager 2.1.0 and 2.6.0. Reflected XSS exists in the carbon part of the product. **CVE ID : CVE-2018-20737**	N/A	A-WSO-API_-040419/389
identity_server					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-03-2019	3.5	An issue was discovered in WSO2 API Manager 2.1.0 and 2.6.0. Reflected XSS exists in the carbon part of the product. **CVE ID : CVE-2018-20737**	N/A	A-WSO-IDEN-040419/390
identity_server_as_key_manager					
N/A	21-03-2019	3.5	An issue was discovered in WSO2 API Manager 2.1.0 and 2.6.0. Reflected XSS exists in the carbon part of the product. **CVE ID : CVE-2018-20737**	N/A	A-WSO-IDEN-040419/391
Xnview					
xnview_mp					
N/A	23-03-2019	6.8	XnView MP 0.93.1 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to VCRUNTIME140!memcpy. **CVE ID : CVE-2019-9962**	N/A	A-XNV-XNVI-040419/392
N/A	23-03-2019	6.8	XnView MP 0.93.1 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to ntdll!RtlFreeHeap. **CVE ID : CVE-2019-9963**	N/A	A-XNV-XNVI-040419/393
N/A	23-03-2019	6.8	XnView MP 0.93.1 on Windows allows remote	N/A	A-XNV-XNVI-040419/394

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to ntdll!RtlpNtMakeTemporaryKey. **CVE ID : CVE-2019-9964**		
N/A	23-03-2019	6.8	XnView MP 0.93.1 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to ntdll!RtlReAllocateHeap. **CVE ID : CVE-2019-9965**	N/A	A-XNV-XNVI-040419/395
xnview_classic					
N/A	23-03-2019	6.8	XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to xnview+0x38536c. **CVE ID : CVE-2019-9966**	N/A	A-XNV-XNVI-040419/396
N/A	23-03-2019	6.8	XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to ntdll!RtlPrefixUnicodeString.	N/A	A-XNV-XNVI-040419/397

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9967		
N/A	23-03-2019	6.8	XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to ntdll!RtlQueueWorkItem. **CVE ID : CVE-2019-9968**	N/A	A-XNV-XNVI-040419/398
N/A	23-03-2019	6.8	XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to xnview+0x385399. **CVE ID : CVE-2019-9969**	N/A	A-XNV-XNVI-040419/399
xpdfreader					
xpdf					
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function PostScriptFunction::exec at Function.cc for the psOpIdiv case. **CVE ID : CVE-2019-10018**	N/A	A-XPD-XPDF-040419/400
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function PSOutputDev::checkPageSlice at PSOutputDev.cc for nStripes. **CVE ID : CVE-2019-10019**	N/A	A-XPD-XPDF-040419/401

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function Splash::scaleImageYuXu at Splash.cc for x Bresenham parameters. **CVE ID : CVE-2019-10020**	N/A	A-XPD-XPDF-040419/402
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function ImageStream::ImageStream at Stream.cc for nComps. **CVE ID : CVE-2019-10021**	N/A	A-XPD-XPDF-040419/403
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is a NULL pointer dereference in the function Gfx::opSetExtGState in Gfx.cc. **CVE ID : CVE-2019-10022**	N/A	A-XPD-XPDF-040419/404
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function PostScriptFunction::exec at Function.cc for the psOpMod case. **CVE ID : CVE-2019-10023**	N/A	A-XPD-XPDF-040419/405
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function Splash::scaleImageYuXu at Splash.cc for y Bresenham parameters. **CVE ID : CVE-2019-10024**	N/A	A-XPD-XPDF-040419/406

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function ImageStream::ImageStream at Stream.cc for nBits. **CVE ID : CVE-2019-10025**	N/A	A-XPD-XPDF-040419/407
N/A	24-03-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an FPE in the function PostScriptFunction::exec in Function.cc for the psOpRoll case. **CVE ID : CVE-2019-10026**	N/A	A-XPD-XPDF-040419/408
N/A	21-03-2019	6.8	There is an invalid memory access vulnerability in the function TextPage::findGaps() located at TextOutputDev.c in Xpdf 4.01, which can (for example) be triggered by sending a crafted pdf file to the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2019-9877**	N/A	A-XPD-XPDF-040419/409
N/A	21-03-2019	6.8	There is an invalid memory access in the function GfxIndexedColorSpace::mapColorToBase() located in GfxState.cc in Xpdf 4.0.0, as used in pdfalto 0.2. It can be triggered by (for	N/A	A-XPD-XPDF-040419/410

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			example) sending a crafted pdf file to the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2019-9878**		
yubico					
libu2f-host					
N/A	21-03-2019	4.6	Yubico libu2f-host 1.1.6 contains unchecked buffers in devs.c, which could enable a malicious token to exploit a buffer overflow. An attacker could use this to attempt to execute malicious code using a crafted USB device masquerading as a security token on a computer where the affected library is currently in use. It is not possible to perform this attack with a genuine YubiKey. **CVE ID : CVE-2018-20340**	https://www.yubico.com/support/security-advisories/ysa-2019-01/	A-YUB-LIBU-040419/411
zeit					
serve					
N/A	21-03-2019	5	A bug in handling the ignore files and directories feature in serve 6.5.3 allows an attacker to read a file or list the directory that the victim has not	N/A	A-ZEI-SERV-040419/412

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowed access to. **CVE ID : CVE-2019-5415**		
N/A	21-03-2019	5	A path traversal vulnerability in serve npm package version 7.0.1 allows the attackers to read content of arbitrary files on the remote server. **CVE ID : CVE-2019-5417**	N/A	A-ZEI-SERV-040419/413
ZNC					
ZNC					
N/A	27-03-2019	4	ZNC before 1.7.3-rc1 allows an existing remote user to cause a Denial of Service (crash) via invalid encoding. **CVE ID : CVE-2019-9917**	N/A	A-ZNC-ZNC-040419/414
Zohocorp					
manageengine_adselfservice_plus					
N/A	21-03-2019	5	An issue was discovered in Zoho ManageEngine ADSelfService Plus 5.x through build 5704. It uses fixed ciphering keys to protect information, giving the capacity for an attacker to decipher any protected data. **CVE ID : CVE-2019-7161**	https://www.manageengine.com/products/self-service-password/release-notes.html	A-ZOH-MANA-040419/415
zzzcms					
zzzphp					
N/A	30-03-2019	7.5	ZZZCMS zzzphp v1.6.3 allows remote attackers to execute arbitrary PHP	N/A	A-ZZZ-ZZZP-040419/416

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟧	code via a .php URL in the plugins/ueditor/php/controller.php?action=catchimage source[] parameter because of a lack of inc/zzz_file.php restrictions. For example, source%5B%5D=http%3A%2F%2F192.168.0.1%2Ftest.php can be used if the 192.168.0.1 web server sends the contents of a .php file (i.e., it does not interpret a .php file). **CVE ID : CVE-2019-10647**		