Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operating System					
Actiontec					
t2200h_firmware					
N/A	17-06-2019	7.2	An issue was discovered on Actiontec T2200H T2200H-31.128L.08 devices, as distributed by Telus. By attaching a UART adapter to the UART pins on the system board, an attacker can use a special key sequence (Ctrl-\) to obtain a shell with root privileges. After gaining root access, the attacker can mount the filesystem read-write and make permanent modifications to the device including bricking of the device, disabling vendor management of the device, preventing automatic upgrades, and permanently installing malicious code on the device. **CVE ID : CVE-2019-12789**	N/A	O-ACT-T220-030719/1
Canonical					
ubuntu_linux					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182,	https://www.synology.com/security/advisory/Synology_SA_19_28	O-CAN-UBUN-030719/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-CAN-UBUN-030719/3
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-CAN-UBUN-030719/4
NULL	19-06-2019	4	Samba 4.10.x before 4.10.5 has a	https://w	O-CAN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			NULL pointer dereference, leading to an AD DC LDAP server Denial of Service. This is related to an attacker using the paged search control. The attacker must have directory read access in order to attempt an exploit. **CVE ID : CVE-2019-12436**	ww.synology.com/security/advisory/Synology_SA_19_27	UBUN-030719/5
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2019	6.9	arch/powerpc/mm/mmu_context_book3s64.c in the Linux kernel before 5.1.15 for powerpc has a bug where unrelated processes may be able to read/write to one another's virtual memory under certain conditions via an mmap above 512 TB. Only a subset of powerpc systems are affected. **CVE ID : CVE-2019-12817**	N/A	O-CAN-UBUN-030719/6
Cisco					
sd-wan_firmware					
N/A	19-06-2019	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution could allow an authenticated, local attacker to elevate lower-level privileges to the root user on an affected device. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow the attacker to make configuration changes to the system as the root user. **CVE ID : CVE-2019-1625**	N/A	O-CIS-SD-W-030719/7
N/A	19-06-2019	6.5	A vulnerability in the vManage web-based UI (Web UI) of the	N/A	O-CIS-SD-W-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco SD-WAN Solution could allow an authenticated, remote attacker to gain elevated privileges on an affected vManage device. The vulnerability is due to a failure to properly authorize certain user actions in the device configuration. An attacker could exploit this vulnerability by logging in to the vManage Web UI and sending crafted HTTP requests to vManage. A successful exploit could allow attackers to gain elevated privileges and make changes to the configuration that they would not normally be authorized to make. **CVE ID : CVE-2019-1626**		030719/8
rv110w_firmware					
Improper Input Validation	19-06-2019	5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to reload the device and causing a	N/A	O-CIS-RV11-030719/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DoS condition. **CVE ID : CVE-2019-1843**		
Improper Authorization	19-06-2019	5	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to disconnect clients that are connected to the guest network on an affected router. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for device disconnection and providing the connected device information. A successful exploit could allow the attacker to deny service to specific clients that are connected to the guest network. **CVE ID : CVE-2019-1897**	N/A	O-CIS-RV11-030719/10
Improper Authorization	19-06-2019	5	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to access the syslog file on an affected device. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for the syslog file. A successful exploit could allow the attacker to access the information contained in the file. **CVE ID : CVE-2019-1898**	N/A	O-CIS-RV11-030719/11
Improper Authorization	19-06-2019	5	A vulnerability in the web interface of Cisco RV110W, RV130W, and RV215W Routers	N/A	O-CIS-RV11-030719/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to acquire the list of devices that are connected to the guest network. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web interface of the router. **CVE ID : CVE-2019-1899**		
rv130w_firmware					
Improper Input Validation	19-06-2019	5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to reload the device and causing a DoS condition. **CVE ID : CVE-2019-1843**	N/A	O-CIS-RV13-030719/13
Improper Authorization	19-06-2019	5	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker	N/A	O-CIS-RV13-030719/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to disconnect clients that are connected to the guest network on an affected router. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for device disconnection and providing the connected device information. A successful exploit could allow the attacker to deny service to specific clients that are connected to the guest network. **CVE ID : CVE-2019-1897**		
Improper Authorization	19-06-2019	5	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to access the syslog file on an affected device. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for the syslog file. A successful exploit could allow the attacker to access the information contained in the file. **CVE ID : CVE-2019-1898**	N/A	O-CIS-RV13-030719/15
Improper Authorization	19-06-2019	5	A vulnerability in the web interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to acquire the list of devices that are connected to the guest network. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a	N/A	O-CIS-RV13-030719/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific URI on the web interface of the router. **CVE ID : CVE-2019-1899**		
rv215w_firmware					
Improper Input Validation	19-06-2019	5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to reload the device and causing a DoS condition. **CVE ID : CVE-2019-1843**	N/A	O-CIS-RV21-030719/17
Improper Authorization	19-06-2019	5	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to disconnect clients that are connected to the guest network on an affected router. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for device disconnection and	N/A	O-CIS-RV21-030719/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			providing the connected device information. A successful exploit could allow the attacker to deny service to specific clients that are connected to the guest network. **CVE ID : CVE-2019-1897**		
Improper Authorization	19-06-2019	5	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to access the syslog file on an affected device. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for the syslog file. A successful exploit could allow the attacker to access the information contained in the file. **CVE ID : CVE-2019-1898**	N/A	O-CIS-RV21-030719/19
Improper Authorization	19-06-2019	5	A vulnerability in the web interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to acquire the list of devices that are connected to the guest network. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web interface of the router. **CVE ID : CVE-2019-1899**	N/A	O-CIS-RV21-030719/20
ios_xe					
Cross-Site Request Forgery	20-06-2019	6.8	A vulnerability in the web-based UI (web UI) of Cisco IOS XE Software could allow an	N/A	O-CIS-IOS_-030719/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web UI on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or reload an affected device. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software with the HTTP Server feature enabled. The default state of the HTTP Server feature is version dependent. **CVE ID : CVE-2019-1904**		
cylan					
clever_dog_smart_camera_panorama_dog-2w_firmware					
Information Exposure	20-06-2019	2.1	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the local network has unauthenticated access to the internal SD card via the HTTP service on port 8000. The HTTP web server on the camera allows anyone to view or download the video archive recorded and saved on the external memory card attached to the device.	N/A	O-CYL-CLEV-030719/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-12919		
Use of Hard-coded Credentials	20-06-2019	10	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the network can login remotely to the camera and gain root access. The device ships with a hardcoded 12345678 password for the root account, accessible from a TELNET login prompt. **CVE ID : CVE-2019-12920**	N/A	O-CYL-CLEV-030719/23
clever_dog_smart_camera_plus_dog-2w-v4_firmware					
Information Exposure	20-06-2019	2.1	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the local network has unauthenticated access to the internal SD card via the HTTP service on port 8000. The HTTP web server on the camera allows anyone to view or download the video archive recorded and saved on the external memory card attached to the device. **CVE ID : CVE-2019-12919**	N/A	O-CYL-CLEV-030719/24
Use of Hard-coded Credentials	20-06-2019	10	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the network can login remotely to the camera and gain root access. The device ships with a hardcoded 12345678 password for the root account, accessible from a TELNET login prompt. **CVE ID : CVE-2019-12920**	N/A	O-CYL-CLEV-030719/25
Debian					
debian_linux					
Improper	17-06-2019	4.3	An issue was discovered in Open	N/A	O-DEB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Ticket Request System (OTRS) 7.0.x through 7.0.7, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. An attacker could send a malicious email to an OTRS system. If a logged-in agent user quotes it, the email could cause the browser to load external image resources. **CVE ID : CVE-2019-12248**		DEBI-030719/26
Deserialization of Untrusted Data	24-06-2019	4.3	FasterXML jackson-databind 2.x before 2.9.9 might allow attackers to have a variety of impacts by leveraging failure to block the logback-core class from polymorphic deserialization. Depending on the classpath content, remote code execution may be possible. **CVE ID : CVE-2019-12384**	https://lists.debian.org/debian-lts-announce/2019/06/msg00019.html	O-DEB-DEBI-030719/27
Information Exposure	17-06-2019	5	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.8, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. In the customer or external frontend, personal information of agents (e.g., Name and mail address) can be disclosed in external notes. **CVE ID : CVE-2019-12497**	https://lists.debian.org/debian-lts-announce/2019/06/msg00004.html	O-DEB-DEBI-030719/28
Information Exposure	19-06-2019	4.3	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x through 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the	https://security.netapp.com/advisory/ntap-20190625-0006/	O-DEB-DEBI-030719/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service has JDOM 1.x or 2.x jar in the classpath, an attacker can send a specifically crafted JSON message that allows them to read arbitrary local files on the server. **CVE ID : CVE-2019-12814**		
genieaccess					
wip3bvaf_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-06-2019	5	Genie Access WIP3BVAF WISH IP 3MP IR Auto Focus Bullet Camera devices through 3.x are vulnerable to directory traversal via the web interface, as demonstrated by reading /etc/shadow. NOTE: this product is discontinued, and its final firmware version has this vulnerability (4.x versions exist only for other Genie Access products). **CVE ID : CVE-2019-7315**	N/A	O-GEN-WIP3-030719/30
Google					
android					
N/A	19-06-2019	7.2	In findAvailSpellCheckerLocked of TextServicesManagerService.java, there is a possible way to bypass the warning dialog when selecting an untrusted spell checker due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0Android ID: A-	N/A	O-GOO-ANDR-030719/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			118694079 **CVE ID : CVE-2019-1985**		
Out-of-bounds Write	19-06-2019	9.3	In ih264d_fmt_conv_420sp_to_420p of ih264d_format_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118399205 **CVE ID : CVE-2019-1989**	N/A	O-GOO-ANDR-030719/32
Out-of-bounds Write	19-06-2019	9.3	In ihevcd_fmt_conv_420sp_to_420p of ihevcd_fmt_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118453553 **CVE ID : CVE-2019-1990**	N/A	O-GOO-ANDR-030719/33
N/A	19-06-2019	9.3	In addLinks of Linkify.java, there is a possible phishing vector due to an unusual root cause. This could lead to remote code execution or misdirection of	N/A	O-GOO-ANDR-030719/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clicks with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116321860 **CVE ID : CVE-2019-2003**		
Information Exposure	19-06-2019	4.9	In publishKeyEvent, publishMotionEvent and sendUnchainedFinishedSignal of InputTransport.cpp, there are uninitialized data leading to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-115739809 **CVE ID : CVE-2019-2004**	N/A	O-GOO-ANDR-030719/35
N/A	19-06-2019	6.8	In onPermissionGrantResult of GrantPermissionsActivity.java, there is a possible incorrectly granted permission due to a missing permission check. This could lead to local escalation of privilege on a locked device with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-68777217 **CVE ID : CVE-2019-2005**	N/A	O-GOO-ANDR-030719/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-06-2019	10	In serviceDied of HalDeathHandlerHidl.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-116665972 **CVE ID : CVE-2019-2006**	N/A	O-GOO-ANDR-030719/37
Integer Overflow or Wraparound	19-06-2019	10	In getReadIndex and getWriteIndex of FifoControllerBase.cpp, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-120789744 **CVE ID : CVE-2019-2007**	N/A	O-GOO-ANDR-030719/38
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-06-2019	7.6	In createEffect of AudioFlinger.cpp, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-122309228 **CVE ID : CVE-2019-2008**	N/A	O-GOO-ANDR-030719/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-06-2019	8.3	In l2c_lcc_proc_pdu of l2c_fcr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120665616 **CVE ID : CVE-2019-2009**	N/A	O-GOO-ANDR-030719/40
Out-of-bounds Write	19-06-2019	7.2	In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118152591 **CVE ID : CVE-2019-2010**	N/A	O-GOO-ANDR-030719/41
Out-of-bounds Write	19-06-2019	7.2	In readNullableNativeHandleNoDup of Parcel.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	N/A	O-GOO-ANDR-030719/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-120084106 **CVE ID : CVE-2019-2011**		
Out-of-bounds Write	19-06-2019	9.3	In rw_t3t_act_handle_fmt_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497437 **CVE ID : CVE-2019-2012**	N/A	O-GOO-ANDR-030719/43
Out-of-bounds Write	19-06-2019	9.3	In rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497583 **CVE ID : CVE-2019-2013**	N/A	O-GOO-ANDR-030719/44
Out-of-bounds Write	19-06-2019	9.3	In rw_t3t_handle_get_sc_poll_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User	N/A	O-GOO-ANDR-030719/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120499324 **CVE ID : CVE-2019-2014**		
Out-of-bounds Write	19-06-2019	9.3	In rw_t3t_act_handle_check_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120503926 **CVE ID : CVE-2019-2015**	N/A	O-GOO-ANDR-030719/46
Out-of-bounds Write	19-06-2019	9.3	In NFA_SendRawFrame of nfa_dm_api.cc, there is a possible out-of-bound write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120664978 **CVE ID : CVE-2019-2016**	N/A	O-GOO-ANDR-030719/47
Out-of-bounds	19-06-2019	7.2	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-121035711 **CVE ID : CVE-2019-2017**		030719/48
N/A	19-06-2019	9.3	In resetPasswordInternal of DevicePolicyManagerService.java , there is a possible bypass of password reset protection due to an unusual root cause. Remote user interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-110172241 **CVE ID : CVE-2019-2018**	N/A	O-GOO-ANDR-030719/49
Out-of-bounds Read	19-06-2019	7.1	In ce_t4t_data_cback of ce_t4t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-115635871 **CVE ID : CVE-2019-2019**	N/A	O-GOO-ANDR-030719/50
Out-of-	19-06-2019	7.1	In llcp_dlc_proc_rr_rnr_pdu of	N/A	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			llcp_dlc.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116788646 **CVE ID : CVE-2019-2020**		ANDR-030719/51
Out-of-bounds Read	19-06-2019	7.1	In rw_t3t_act_handle_ndef_detect_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120428041 **CVE ID : CVE-2019-2021**	N/A	O-GOO-ANDR-030719/52
Out-of-bounds Read	19-06-2019	7.1	In rw_t3t_act_handle_fmt_rsp and rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2	N/A	O-GOO-ANDR-030719/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android-8.0 Android-8.1 Android-9Android ID: A-120506143 **CVE ID : CVE-2019-2022**		
N/A	19-06-2019	7.2	In ServiceManager::add function in the hardware service manager, there is an insecure permissions check based on the PID of the caller. This could allow an app to add or replace a HAL service with its own service, gaining code execution in a privileged process.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-121035042Upstream kernel **CVE ID : CVE-2019-2023**	N/A	O-GOO-ANDR-030719/54
Use After Free	19-06-2019	7.2	In em28xx_unregister_dvb of em28xx-dvb.c, there is a possible use after free issue. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-111761954References: Upstream kernel **CVE ID : CVE-2019-2024**	N/A	O-GOO-ANDR-030719/55
Use After Free	19-06-2019	7.2	In binder_thread_read of binder.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	N/A	O-GOO-ANDR-030719/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android kernelAndroid ID: A-116855682References: Upstream kernel **CVE ID : CVE-2019-2025**		
Linksys					
wrt1900acs_firmware					
N/A	17-06-2019	5	An issue was discovered on Linksys WRT1900ACS 1.0.3.187766 devices. An ability exists for an unauthenticated user to browse a confidential ui/1.0.99.187766/dynamic/js/setup.js.localized file on the router's webserver, allowing for an attacker to identify possible passwords that the system uses to set the default guest network password. An attacker can use this list of 30 words along with a random 2 digit number to brute force their access onto a router's guest network. **CVE ID : CVE-2019-7579**	N/A	O-LIN-WRT1-030719/57
Linux					
linux_kernel					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd	https://www.synology.com/security/advisory/Synology_SA_19_28	O-LIN-LINU-030719/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			88ed1a2f78cff. **CVE ID : CVE-2019-11477**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-LIN-LINU-030719/59
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-LIN-LINU-030719/60
Improper Restriction of Operations	25-06-2019	6.9	arch/powerpc/mm/mmu_context_book3s64.c in the Linux kernel before 5.1.15 for powerpc has a bug where unrelated processes	N/A	O-LIN-LINU-030719/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			may be able to read/write to one another's virtual memory under certain conditions via an mmap above 512 TB. Only a subset of powerpc systems are affected. **CVE ID : CVE-2019-12817**		
NULL Pointer Dereference	18-06-2019	4.6	i915_gem_userptr_get_pages in drivers/gpu/drm/i915/i915_gem_userptr.c in the Linux kernel 4.15.0 on Ubuntu 18.04.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact via crafted ioctl calls to /dev/dri/card0. **CVE ID : CVE-2019-12881**	N/A	O-LIN-LINU-030719/62
NULL Pointer Dereference	26-06-2019	4.3	A NULL pointer dereference vulnerability in the function nfc_genl_deactivate_target() in net/nfc/netlink.c in the Linux kernel before 5.1.13 can be triggered by a malicious user-mode program that omits certain NFC attributes, leading to denial of service. **CVE ID : CVE-2019-12984**	N/A	O-LIN-LINU-030719/63
Double Free	18-06-2019	7.2	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS). **CVE ID : CVE-2019-3896**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3896	O-LIN-LINU-030719/64
Netgear					
r7900_firmware					
Informatio	17-06-2019	6.4	An exploitable arbitrary memory	N/A	O-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Exposure			read vulnerability exists in the KCodes NetUSB.ko kernel module which enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. A specially crafted index value can cause an invalid memory read, resulting in a denial of service or remote information disclosure. An unauthenticated attacker can send a crafted packet on the local network to trigger this vulnerability. **CVE ID : CVE-2019-5016**		R790-030719/65
r8000_firmware					
Information Exposure	17-06-2019	6.4	An exploitable arbitrary memory read vulnerability exists in the KCodes NetUSB.ko kernel module which enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. A specially crafted index value can cause an invalid memory read, resulting in a denial of service or remote information disclosure. An unauthenticated attacker can send a crafted packet on the local network to trigger this vulnerability. **CVE ID : CVE-2019-5016**	N/A	O-NET-R800-030719/66
Information Exposure	17-06-2019	5	An exploitable information disclosure vulnerability exists in the KCodes NetUSB.ko kernel module that enables the ReadySHARE Printer functionality of at least two	N/A	O-NET-R800-030719/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NETGEAR Nighthawk Routers and potentially several other vendors/products. An unauthenticated, remote attacker can craft and send a packet containing an opcode that will trigger the kernel module to return several addresses. One of which can be used to calculate the dynamic base address of the module for further exploitation. **CVE ID : CVE-2019-5017**		
pix-link					
lv-wr09_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2019	4.3	An XSS issue on the PIX-Link Repeater/Router LV-WR09 with firmware v28K.MiniRouter.20180616 allows attackers to steal credentials without being connected to the network. The attack vector is a crafted ESSID. **CVE ID : CVE-2019-12933**	N/A	O-PIX-LV-W-030719/68
Redhat					
enterprise_linux_aus					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			88ed1a2f78cff. **CVE ID : CVE-2019-11477**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/70
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/71
enterprise_linux_eus					
Integer Overflow or	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject	https://www.synology.com/	O-RED-ENTE-030719/72

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	security/advisory/Synology_SA_19_28	
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/73
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**		
enterprise_linux_desktop					
Double Free	18-06-2019	7.2	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS). **CVE ID : CVE-2019-3896**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3896	O-RED-ENTE-030719/75
enterprise_linux_server					
Double Free	18-06-2019	7.2	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS). **CVE ID : CVE-2019-3896**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3896	O-RED-ENTE-030719/76
enterprise_linux_server_aus					
Double Free	18-06-2019	7.2	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS). **CVE ID : CVE-2019-3896**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3896	O-RED-ENTE-030719/77
enterprise_linux_workstation					
Double Free	18-06-2019	7.2	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can	https://bugzilla.redhat.com/show_bu	O-RED-ENTE-030719/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use this flaw for a privilege escalation or for a system crash and a denial of service (DoS). **CVE ID : CVE-2019-3896**	g.cgi?id=CVE-2019-3896	
virtualization					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-VIRT-030719/79
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-VIRT-030719/80
Uncontrolled Resource	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This	https://www.synology.com/	O-RED-VIRT-030719/81

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	security/advisory/Synology_SA_19_28	
enterprise_linux					
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2019	9	PostgreSQL versions 10.x before 10.9 and versions 11.x before 11.4 are vulnerable to a stack-based buffer overflow. Any authenticated user can overflow a stack-based buffer by changing the user's own password to a purpose-crafted value. This often suffices to execute arbitrary code as the PostgreSQL operating system account. **CVE ID : CVE-2019-10164**	N/A	O-RED-ENTE-030719/82
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			88ed1a2f78cff. **CVE ID : CVE-2019-11477**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/84
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	O-RED-ENTE-030719/85
toaruos					
toaruos					
Improper Restriction	23-06-2019	7.2	apps/gsudo.c in gsudo in ToaruOS through 1.10.9 has a	N/A	O-TOA-TOAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			buffer overflow allowing local privilege escalation to the root user via the DISPLAY environment variable. **CVE ID : CVE-2019-12937**		030719/86
Tp-link					
tl-wr1043nd_firmware					
Improper Authentication	19-06-2019	10	An issue was discovered on TP-Link TL-WR1043ND V2 devices. An attacker can send a cookie in an HTTP authentication packet to the router management web interface, and fully control the router without knowledge of the credentials. **CVE ID : CVE-2019-6971**	N/A	O-TP--TL-W-030719/87
N/A	19-06-2019	5	An issue was discovered on TP-Link TL-WR1043ND V2 devices. The credentials can be easily decoded and cracked by brute-force, WordList, or Rainbow Table attacks. Specifically, credentials in the "Authorization" cookie are encoded with URL encoding and base64, leading to easy decoding. Also, the username is cleartext, and the password is hashed with the MD5 algorithm (after decoding of the URL encoded string with base64). **CVE ID : CVE-2019-6972**	N/A	O-TP--TL-W-030719/88
Zyxel					
uag2100_firmware					
Improper Neutralization of Input	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG,	N/A	O-ZYX-UAG2-030719/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**		
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-UAG2-030719/90
uag4100_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**	N/A	O-ZYX-UAG4-030719/91
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-UAG4-030719/92
uag5100_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**	N/A	O-ZYX-UAG5-030719/93
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-UAG5-030719/94
zywall_vpn100_firmware					
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-ZYWA-030719/95
zywall_vpn300_firmware					
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the	https://www.zyxel.com/support/vulnerabilities-related-	O-ZYX-ZYWA-030719/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	to-the-Free-Time-feature.shtml	
usg1100_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**	N/A	O-ZYX-USG1-030719/97
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-USG1-030719/98
usg110_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**	N/A	O-ZYX-USG1-030719/99
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and	https://www.zyxel.com/supp	O-ZYX-USG1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	ort/vulnerabilities-related-to-the-Free-Time-feature.shtml	030719/100
usg1900_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**	N/A	O-ZYX-USG1-030719/101
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-USG1-030719/102
usg210_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**	N/A	O-ZYX-USG2-030719/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-USG2-030719/104
usg2200-vpn_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**	N/A	O-ZYX-USG2-030719/105
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-USG2-030719/106
usg310_firmware					
Improper Neutralization of Input During Web Page	27-06-2019	4.3	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web	N/A	O-ZYX-USG3-030719/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			script or HTML via the err_msg parameter. **CVE ID : CVE-2019-12581**		
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-USG3-030719/108
zywall_1100_firmware					
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-ZYWA-030719/109
zywall_110_firmware					
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-ZYWA-030719/110
zywall_310_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-06-2019	6.4	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service. **CVE ID : CVE-2019-12583**	https://www.zyxel.com/support/vulnerabilities-related-to-the-Free-Time-feature.shtml	O-ZYX-ZYWA-030719/111
Application					
Advantech					
webaccess					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2019	7.5	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 10012 RPC call. **CVE ID : CVE-2019-3953**	N/A	A-ADV-WEBA-030719/112
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2019	7.5	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 81024 RPC call. **CVE ID : CVE-2019-3954**	N/A	A-ADV-WEBA-030719/113
afian					
filerun					
Improper Neutralization of Input During Web Page	20-06-2019	4.3	FileRun 2019.05.21 allows XSS via the filename to the ?module=fileman&section=do&page=up URI. **CVE ID : CVE-2019-12905**	N/A	A-AFI-FILE-030719/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')					
alpinelinux					
abuild					
N/A	18-06-2019	4	Alpine Linux abuild through 3.4.0 allows an unprivileged member of the abuild group to add an untrusted package via a --keys-dir option that causes acceptance of an untrusted signing key. **CVE ID : CVE-2019-12875**	https://security.netapp.com/advisory/ntap-20190625-0005/	A-ALP-ABUI-030719/115
alternate-tools					
alternate_pic_view					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-06-2019	5	Alternate Pic View 2.600 has a User Mode Write AV starting at PicViewer!PerfgrapFinalize+0x00000000000a8868. **CVE ID : CVE-2019-12893**	N/A	A-ALT-ALTE-030719/116
Improper Access Control	19-06-2019	5	Alternate Pic View 2.600 has a Read Access Violation at the Instruction Pointer after a call from PicViewer!PerfgrapFinalize+0x00000000000a9a1b. **CVE ID : CVE-2019-12894**	N/A	A-ALT-ALTE-030719/117
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-06-2019	5	In Alternate Pic View 2.600, the Exception Handler Chain is Corrupted starting at PicViewer!PerfgrapFinalize+0x00000000000b916d. **CVE ID : CVE-2019-12895**	N/A	A-ALT-ALTE-030719/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
analogic					
poste.io					
Protection Mechanism Failure	24-06-2019	4	The Roundcube component of Analogic Poste.io 2.1.6 uses .htaccess to protect the logs/ folder, which is effective with the Apache HTTP Server but is ineffective with nginx. Attackers can read logs via the webmail/logs/sendmail URI. **CVE ID : CVE-2019-12938**	N/A	A-ANA-POST-030719/119
Apache					
tomcat					
Uncontrolled Resource Consumption	21-06-2019	5	The fix for CVE-2019-0199 was incomplete and did not address HTTP/2 connection window exhaustion on write in Apache Tomcat versions 9.0.0.M1 to 9.0.19 and 8.5.0 to 8.5.40 . By not sending WINDOW_UPDATE messages for the connection window (stream 0) clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS. **CVE ID : CVE-2019-10072**	https://www.synology.com/security/advisory/Synology_SA_19_29	A-APA-TOMC-030719/120
allura					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2019	4.3	In Apache Allura prior to 1.11.0, a vulnerability exists for stored XSS on the user dropdown selector when creating or editing tickets. The XSS executes when a user engages with that dropdown on that page. **CVE ID : CVE-2019-10085**	N/A	A-APA-ALLU-030719/121
Atlassian					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jira					
Improper Access Control	26-06-2019	4	The issue searching component in Jira before version 8.1.0 allows remote attackers to deny access to Jira service via denial of service vulnerability in issue search when ordering by "Epic Name". **CVE ID : CVE-2019-11583**	N/A	A-ATL-JIRA-030719/122
bcnquark					
quarking_password_manager					
Improper Input Validation	24-06-2019	4.3	BCN Quark Quarking Password Manager 3.1.84 suffers from a clickjacking vulnerability caused by allowing * within web_accessible_resources. An attacker can take advantage of this vulnerability and cause significant harm. **CVE ID : CVE-2019-12880**	N/A	A-BCN-QUAR-030719/123
Bzip					
bzip2					
Out-of-bounds Write	19-06-2019	7.5	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors. **CVE ID : CVE-2019-12900**	N/A	A-BZI-BZIP-030719/124
Cesanta					
mongoose					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-06-2019	7.5	An issue was discovered in Mongoose before 6.15. The parse_mqtt() function in mg_mqtt.c has a critical heap-based buffer overflow. **CVE ID : CVE-2019-12951**	N/A	A-CES-MONG-030719/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cisco					
data_center_network_manager					
Improper Access Control	26-06-2019	7.5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device. The vulnerability is due to improper session management on affected DCNM software. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device. **CVE ID : CVE-2019-1619**	N/A	A-CIS-DATA-030719/126
N/A	26-06-2019	10	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to upload arbitrary files on an affected device. The vulnerability is due to incorrect permission settings in affected DCNM software. An attacker could exploit this vulnerability by uploading specially crafted data to the affected device. A successful exploit could allow the attacker to write arbitrary files on the filesystem and execute code with root privileges on the affected device.	N/A	A-CIS-DATA-030719/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1620		
N/A	26-06-2019	5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to gain access to sensitive files on an affected device. The vulnerability is due to incorrect permissions settings on affected DCNM software. An attacker could exploit this vulnerability by connecting to the web-based management interface of an affected device and requesting specific URLs. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device. **CVE ID : CVE-2019-1621**	N/A	A-CIS-DATA-030719/128
Improper Access Control	26-06-2019	5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to retrieve sensitive information from an affected device. The vulnerability is due to improper access controls for certain URLs on affected DCNM software. An attacker could exploit this vulnerability by connecting to the web-based management interface of an affected device and requesting specific URLs. A successful exploit could allow the attacker to download log files and diagnostic information from the affected device.	N/A	A-CIS-DATA-030719/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1622		
integrated_management_controller					
Information Exposure	19-06-2019	4	A vulnerability in the Server Utilities of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to gain unauthorized access to sensitive user information from the configuration data that is stored on the affected system. The vulnerability is due to insufficient protection of data in the configuration file. An attacker could exploit this vulnerability by downloading the configuration file. An exploit could allow the attacker to use the sensitive information from the file to elevate privileges. **CVE ID : CVE-2019-1627**	N/A	A-CIS-INTE-030719/130
Integer Underflow (Wrap or Wraparound)	19-06-2019	2.1	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect bounds checking. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. An exploit could allow the attacker to cause a buffer overflow, resulting in a process crash and DoS condition on the device. **CVE ID : CVE-2019-1628**	N/A	A-CIS-INTE-030719/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	19-06-2019	5	A vulnerability in the configuration import utility of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to have write access and upload arbitrary data to the filesystem. The vulnerability is due to a failure to delete temporarily uploaded files. An attacker could exploit this vulnerability by crafting a malicious file and uploading it to the affected device. An exploit could allow the attacker to fill up the filesystem or upload malicious scripts. **CVE ID : CVE-2019-1629**	N/A	A-CIS-INTE-030719/132
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-06-2019	2.1	A vulnerability in the firmware signature checking program of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient checking of an input buffer. An attacker could exploit this vulnerability by passing a crafted file to the affected system. A successful exploit could inhibit an administrator's ability to access the system. **CVE ID : CVE-2019-1630**	N/A	A-CIS-INTE-030719/133
Missing Authentication for Critical Function	19-06-2019	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to access potentially sensitive	N/A	A-CIS-INTE-030719/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system usage information. The vulnerability is due to a lack of proper data protection mechanisms. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow an attacker to view sensitive system data. **CVE ID : CVE-2019-1631**		
Cross-Site Request Forgery (CSRF)	19-06-2019	6	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on the affected device. **CVE ID : CVE-2019-1632**	N/A	A-CIS-INTE-030719/135
Improper Neutralization of Special Elements used in an OS Command	19-06-2019	7.2	A vulnerability in the CLI of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient validation of user-	N/A	A-CIS-INTE-030719/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			supplied input at the CLI. An attacker could exploit this vulnerability by authenticating with the administrator password via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute arbitrary commands on the device with root privileges. **CVE ID : CVE-2019-1879**		
prime_service_catalog					
Cross-Site Request Forgery (CSRF)	19-06-2019	6.8	A vulnerability in the web-based management interface of Cisco Prime Service Catalog Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protection mechanisms on the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. **CVE ID : CVE-2019-1874**	N/A	A-CIS-PRIM-030719/137
Improper Neutralization of Input During Web Page Generation	19-06-2019	3.5	A vulnerability in the web-based management interface of Cisco Prime Service Catalog could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The	N/A	A-CIS-PRIM-030719/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by adding specific strings to multiple configuration fields. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. **CVE ID : CVE-2019-1875**		
wide_area_application_services					
Missing Authentication for Critical Function	19-06-2019	5	A vulnerability in the HTTPS proxy feature of Cisco Wide Area Application Services (WAAS) Software could allow an unauthenticated, remote attacker to use the Central Manager as an HTTPS proxy. The vulnerability is due to insufficient authentication of proxy connection requests. An attacker could exploit this vulnerability by sending a malicious HTTPS CONNECT message to the Central Manager. A successful exploit could allow the attacker to access public internet resources that would normally be blocked by corporate policies. **CVE ID : CVE-2019-1876**	N/A	A-CIS-WIDE-030719/139
security_manager					
Improper Restriction of XML External	19-06-2019	6.4	A vulnerability in Cisco Security Manager could allow an unauthenticated, remote attacker to access sensitive information or	N/A	A-CIS-SECU-030719/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference ('XXE')			cause a denial of service (DoS) condition. The vulnerability is due to improper restrictions on XML entities. An attacker could exploit this vulnerability by sending malicious requests to a targeted system that contain references within XML entities. An exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a DoS condition. **CVE ID : CVE-2019-1903**		
unified_computing_system					
Information Exposure	19-06-2019	4	A vulnerability in the Server Utilities of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to gain unauthorized access to sensitive user information from the configuration data that is stored on the affected system. The vulnerability is due to insufficient protection of data in the configuration file. An attacker could exploit this vulnerability by downloading the configuration file. An exploit could allow the attacker to use the sensitive information from the file to elevate privileges. **CVE ID : CVE-2019-1627**	N/A	A-CIS-UNIF-030719/141
Integer Underflow (Wrap or	19-06-2019	2.1	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an	N/A	A-CIS-UNIF-030719/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect bounds checking. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. An exploit could allow the attacker to cause a buffer overflow, resulting in a process crash and DoS condition on the device. **CVE ID : CVE-2019-1628**		
Missing Authentication for Critical Function	19-06-2019	5	A vulnerability in the configuration import utility of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to have write access and upload arbitrary data to the filesystem. The vulnerability is due to a failure to delete temporarily uploaded files. An attacker could exploit this vulnerability by crafting a malicious file and uploading it to the affected device. An exploit could allow the attacker to fill up the filesystem or upload malicious scripts. **CVE ID : CVE-2019-1629**	N/A	A-CIS-UNIF-030719/143
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-06-2019	2.1	A vulnerability in the firmware signature checking program of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is	N/A	A-CIS-UNIF-030719/144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient checking of an input buffer. An attacker could exploit this vulnerability by passing a crafted file to the affected system. A successful exploit could inhibit an administrator's ability to access the system. **CVE ID : CVE-2019-1630**		
Missing Authentication for Critical Function	19-06-2019	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to access potentially sensitive system usage information. The vulnerability is due to a lack of proper data protection mechanisms. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow an attacker to view sensitive system data. **CVE ID : CVE-2019-1631**	N/A	A-CIS-UNIF-030719/145
Cross-Site Request Forgery (CSRF)	19-06-2019	6	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user to follow a	N/A	A-CIS-UNIF-030719/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on the affected device. **CVE ID : CVE-2019-1632**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-06-2019	7.2	A vulnerability in the CLI of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient validation of user-supplied input at the CLI. An attacker could exploit this vulnerability by authenticating with the administrator password via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute arbitrary commands on the device with root privileges. **CVE ID : CVE-2019-1879**	N/A	A-CIS-UNIF-030719/147
email_security_appliance					
Improper Input Validation	19-06-2019	5	A vulnerability in the GZIP decompression engine of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper validation of GZIP-formatted files. An attacker could exploit this vulnerability by sending a malicious file inside a crafted	N/A	A-CIS-EMAI-030719/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GZIP-compressed file. A successful exploit could allow the attacker to bypass configured content filters that would normally drop the email. **CVE ID : CVE-2019-1905**		
prime_infrastructure					
N/A	19-06-2019	4	A vulnerability in the Virtual Domain system of Cisco Prime Infrastructure (PI) could allow an authenticated, remote attacker to change the virtual domain configuration, which could lead to privilege escalation. The vulnerability is due to improper validation of API requests. An attacker could exploit this vulnerability by manipulating requests sent to an affected PI server. A successful exploit could allow the attacker to change the virtual domain configuration and possibly elevate privileges. **CVE ID : CVE-2019-1906**	N/A	A-CIS-PRIM-030719/149
meeting_server					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-06-2019	7.2	A vulnerability in the CLI configuration shell of Cisco Meeting Server could allow an authenticated, local attacker to inject arbitrary commands as the root user. The vulnerability is due to insufficient input validation during the execution of a vulnerable CLI command. An attacker with administrator-level credentials could exploit this vulnerability by injecting crafted arguments during command execution. A successful exploit	N/A	A-CIS-MEET-030719/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to perform arbitrary code execution as root on an affected product. **CVE ID : CVE-2019-1623**		
Citrix					
appdna					
Improper Access Control	24-06-2019	7.5	Citrix AppDNA before 7 1906.1.0.472 has Incorrect Access Control. **CVE ID : CVE-2019-12292**	N/A	A-CIT-APPD-030719/151
Corel					
paintshop_pro_2019					
Integer Overflow or Wraparound	19-06-2019	6.8	An issue was discovered in Corel PaintShop Pro 2019 21.0.0.119. An integer overflow in the jp2 parsing library allows an attacker to overwrite memory and to execute arbitrary code. **CVE ID : CVE-2019-6114**	N/A	A-COR-PAIN-030719/152
Craftcms					
craft_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2019	4.3	Craft CMS 3.1.30 has XSS. **CVE ID : CVE-2019-12823**	https://github.com/craftcms/cms/commit/6432eca59b93bcea2ca2616199e5d419447e613f	A-CRA-CRAF-030719/153
Dell					
supportassist_for_business_pcs					
Uncontrolled Search Path	25-06-2019	6.8	PC-Doctor Toolbox before 7.3 has an Uncontrolled Search Path Element.	N/A	A-DEL-SUPP-030719/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Element			**CVE ID : CVE-2019-12280**		
N/A	20-06-2019	7.2	Dell SupportAssist for Business PCs version 2.0 and Dell SupportAssist for Home PCs version 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, and 3.2.1 contain an Improper Privilege Management Vulnerability. A malicious local user can exploit this vulnerability by inheriting a system thread using a leaked thread handle to gain system privileges on the affected machine. **CVE ID : CVE-2019-3735**	N/A	A-DEL-SUPP-030719/155
supportassist_for_home_pcs					
Uncontrolled Search Path Element	25-06-2019	6.8	PC-Doctor Toolbox before 7.3 has an Uncontrolled Search Path Element. **CVE ID : CVE-2019-12280**	N/A	A-DEL-SUPP-030719/156
N/A	20-06-2019	7.2	Dell SupportAssist for Business PCs version 2.0 and Dell SupportAssist for Home PCs version 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, and 3.2.1 contain an Improper Privilege Management Vulnerability. A malicious local user can exploit this vulnerability by inheriting a system thread using a leaked thread handle to gain system privileges on the affected machine. **CVE ID : CVE-2019-3735**	N/A	A-DEL-SUPP-030719/157
avamar_data_migration_enabler_web_interface					
Improper Input Validation	19-06-2019	5	Dell EMC Avamar ADMe Web Interface 1.0.50 and 1.0.51 are affected by an LFI vulnerability	N/A	A-DEL-AVAM-030719/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which may allow a malicious user to download arbitrary files from the affected system by sending a specially crafted request to the Web Interface application. **CVE ID : CVE-2019-3737**		
deltaww					
devicenet_builder					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-06-2019	7.5	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at image00400000+0x000000000017a45e. **CVE ID : CVE-2019-12898**	N/A	A-DEL-DEVI-030719/159
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-06-2019	7.5	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at ntdll!RtlQueueWorkItem+0x00000000000005e3. **CVE ID : CVE-2019-12899**	N/A	A-DEL-DEVI-030719/160
Dotcms					
dotcms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-06-2019	6.5	dotCMS before 5.1.6 is vulnerable to a SQL injection that can be exploited by an attacker of the role Publisher via view_unpushed_bundles.jsp. **CVE ID : CVE-2019-12872**	N/A	A-DOT-DOTC-030719/161
Dotnetblogengine					
blogengine.net					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference ('XXE')	21-06-2019	5	BlogEngine.NET 3.3.7.0 and earlier allows XML External Entity Blind Injection, related to pingback.axd and BlogEngine.Core/Web/HttpHandlers/PingbackHandler.cs. **CVE ID : CVE-2019-10718**	N/A	A-DOT-BLOG-030719/162
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-06-2019	6.5	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution because file creation is mishandled, related to /api/upload and BlogEngine.NET/AppCode/Api/UploadController.cs. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714. **CVE ID : CVE-2019-10719**	N/A	A-DOT-BLOG-030719/163
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-06-2019	6.5	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution via the theme cookie to the File Manager. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714. **CVE ID : CVE-2019-10720**	N/A	A-DOT-BLOG-030719/164
Improper Restriction of XML External Entity Reference ('XXE')	21-06-2019	5	BlogEngine.NET 3.3.7 and earlier allows XXE via an apml file to syndication.axd. **CVE ID : CVE-2019-11392**	N/A	A-DOT-BLOG-030719/165
edrawsoft					
edraw_max					
Improper Restriction	19-06-2019	5	Edraw Max 7.9.3 has Heap Corruption starting at	N/A	A-EDR-EDRA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			ntdll!RtlpNtMakeTemporaryKey+0x0000000000001a77. **CVE ID : CVE-2019-12896**		030719/166
Improper Access Control	19-06-2019	5	Edraw Max 7.9.3 has a Read Access Violation at the Instruction Pointer after a call from ObjectModule!Paint::Clear+0x0000000000000074. **CVE ID : CVE-2019-12897**	N/A	A-EDR-EDRA-030719/167
exacq					
enterprise_system_manager					
Improper Authorization	18-06-2019	6.9	A vulnerability in the exacqVision Enterprise System Manager (ESM) v5.12.2 application whereby unauthorized privilege escalation can potentially be achieved. This vulnerability impacts exacqVision ESM v5.12.2 and all prior versions of ESM running on a Windows operating system. This issue does not impact any Windows Server OSs, or Linux deployments with permissions that are not inherited from the root directory. Authorized Users have ?modify? permission to the ESM folders, which allows a low privilege account to modify files located in these directories. An executable can be renamed and replaced by a malicious file that could connect back to a bad actor providing system level privileges. A low privileged user is not able to restart the service, but a restart	https://www.johnsoncontrols.com/-/media/jci/be/united-states/specialty-pages/product-security/files/cpp-psa-2019-01-v2-exacqvision-esm.pdf	A-EXA-ENTE-030719/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the system would trigger the execution of the malicious file. This issue affects: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) Version 5.12.2 and prior versions; This issue does not affect: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) 19.03 and above. **CVE ID : CVE-2019-7588**		
F5					
traffix_sdc					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-TRAF-030719/169
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182,	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-TRAF-030719/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**		
big-ip_access_policy_manager					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/171
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/172
Uncontrolled	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is	https://www.synol	A-F5-BIG--030719/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	ogy.com/security/advisory/Synology_SA_19_28	
big-ip_advanced_firewall_manager					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/174
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/176
big-ip_analytics					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11477		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/178
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/179
big-ip_application_acceleration_manager					
Integer Overflow or Wraparou	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the	https://www.synology.com/security/	A-F5-BIG--030719/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nd			Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	advisory/ Synology_ SA_19_28	
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/181
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**		
big-ip_application_security_manager					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/183
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/184
Uncontrolled Resource	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This	https://www.synology.com/	A-F5-BIG--030719/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	security/advisory/Synology_SA_19_28	
big-ip_domain_name_system					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/186
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/188
big-ip_edge_gateway					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/190
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/191
big-ip_fraud_protection_service					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments	https://www.synology.com/security/advisory/Synology_	A-F5-BIG--030719/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	SA_19_28	
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/193
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			b4654b9fc363. **CVE ID : CVE-2019-11479**		
big-ip_global_traffic_manager					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/195
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/196
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly	https://www.synology.com/security/advisory/	A-F5-BIG--030719/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	Synology_SA_19_28	
big-ip_link_controller					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/198
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11,	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/200
big-ip_local_traffic_manager					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/201
Uncontrolled	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue	https://www.synol	A-F5-BIG--030719/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	ogy.com/security/advisory/Synology_SA_19_28	
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/203
big-ip_policy_enforcement_manager					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/205
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11479		
big-ip_webaccelerator					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/207
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-F5-BIG--030719/208
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were	https://www.synology.com/security/advisory/Synology_	A-F5-BIG--030719/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	SA_19_28	
Fasterxml					
jackson-databind					
Deserialization of Untrusted Data	24-06-2019	4.3	FasterXML jackson-databind 2.x before 2.9.9 might allow attackers to have a variety of impacts by leveraging failure to block the logback-core class from polymorphic deserialization. Depending on the classpath content, remote code execution may be possible. **CVE ID : CVE-2019-12384**	https://lists.debian.org/debian-lts-announce/2019/06/msg00019.html	A-FAS-JACK-030719/210
Information Exposure	19-06-2019	4.3	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x through 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has JDOM 1.x or 2.x jar in the classpath, an attacker can send a specifically crafted JSON message that allows them to read arbitrary local files on the server. **CVE ID : CVE-2019-12814**	https://security.netapp.com/advisory/ntap-20190625-0006/	A-FAS-JACK-030719/211
fusionpbx					
fusionpbx					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-06-2019	4	app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 suffers from an information disclosure vulnerability due to excessive debug information, which allows authenticated administrative attackers to obtain credentials and other sensitive information. **CVE ID : CVE-2019-11407**	N/A	A-FUS-FUSI-030719/212
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-06-2019	4.3	XSS in app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 allows remote unauthenticated attackers to inject arbitrary JavaScript characters by placing a phone call using a specially crafted caller ID number. This can further lead to remote code execution by chaining this vulnerability with a command injection vulnerability also present in FusionPBX. **CVE ID : CVE-2019-11408**	N/A	A-FUS-FUSI-030719/213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-06-2019	6.5	app/operator_panel/exec.php in the Operator Panel module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation that allows authenticated non-administrative attackers to execute commands on the host. This can further lead to remote code execution when combined with an XSS vulnerability also present in the FusionPBX Operator Panel module. **CVE ID : CVE-2019-11409**	N/A	A-FUS-FUSI-030719/214
Improper	17-06-2019	9	app/backup/index.php in the	N/A	A-FUS-FUSI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			Backup Module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation, which allows authenticated administrative attackers to execute commands on the host. **CVE ID : CVE-2019-11410**		030719/215
glyphandcog					
xpdfreader					
Out-of-bounds Read	24-06-2019	6.8	In Xpdf 4.01.01, a buffer over-read could be triggered in FoFiType1C::convertToType1 in fofi/FoFiType1C.cc when the index number is larger than the charset array bounds. It can, for example, be triggered by sending a crafted PDF document to the pdftops tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact. **CVE ID : CVE-2019-12957**	N/A	A-GLY-XPDF-030719/216
Out-of-bounds Read	24-06-2019	4.3	In Xpdf 4.01.01, a heap-based buffer over-read could be triggered in FoFiType1C::convertToType0 in fofi/FoFiType1C.cc when it is trying to access the second privateDicts array element, because the privateDicts array has only one element allocated. **CVE ID : CVE-2019-12958**	N/A	A-GLY-XPDF-030719/217
GNU					
binutils					
Out-of-	26-06-2019	4.3	An issue was discovered in the	N/A	A-GNU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. There is a heap-based buffer over-read in _bfd_doprnt in bfd.c because elf_object_p in elfcode.h mishandles an e_shstrndx section of type SHT_GROUP by omitting a trailing '\0' character. **CVE ID : CVE-2019-12972**		BINU-030719/218
Gnupg					
libgcrypt					
N/A	19-06-2019	4.3	In Libgcrypt 1.8.4, the C implementation of AES is vulnerable to a flush-and-reload side-channel attack because physical addresses are available to other processes. (The C implementation is used on platforms where an assembly-language implementation is unavailable.) **CVE ID : CVE-2019-12904**	N/A	A-GNU-LIBG-030719/219
Google					
chrome					
Use After Free	27-06-2019	6.8	Use after free in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2019-5808**	N/A	A-GOO-CHRO-030719/220
Use After Free	27-06-2019	6.8	Use after free in file chooser in Google Chrome prior to 74.0.3729.108 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted	N/A	A-GOO-CHRO-030719/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML page. **CVE ID : CVE-2019-5809**		
Information Exposure	27-06-2019	4.3	Information leak in autofill in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2019-5810**	N/A	A-GOO-CHRO-030719/222
Use After Free	27-06-2019	6.8	Use after free in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2019-5813**	N/A	A-GOO-CHRO-030719/223
N/A	27-06-2019	4.3	Incorrect security UI in popup blocker in Google Chrome on iOS prior to 75.0.3770.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2019-5840**	N/A	A-GOO-CHRO-030719/224
HP					
support_assistant					
N/A	25-06-2019	7.2	HP Support Assistant 8.7.50 and earlier allows a user to gain system privilege and allows unauthorized modification of directories or files. Note: A different vulnerability than CVE-2019-6329. **CVE ID : CVE-2019-6328**	https://support.hp.com/us-en/document/c06388027	A-HP-SUPP-030719/225
N/A	25-06-2019	7.2	HP Support Assistant 8.7.50 and earlier allows a user to gain system privilege and allows	https://support.hp.com/us-	A-HP-SUPP-030719/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized modification of directories or files. Note: A different vulnerability than CVE-2019-6328. **CVE ID : CVE-2019-6329**	en/document/c06388027	
IBM					
rational_collaborative_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157383. **CVE ID : CVE-2019-4083**	N/A	A-IBM-RATI-030719/227
Information Exposure	27-06-2019	4	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384. **CVE ID : CVE-2019-4084**	N/A	A-IBM-RATI-030719/228
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-06-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure	N/A	A-IBM-RATI-030719/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			within a trusted session. IBM X-Force ID: 159647. **CVE ID : CVE-2019-4249**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159648. **CVE ID : CVE-2019-4250**	N/A	A-IBM-RATI-030719/230
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883. **CVE ID : CVE-2019-4252**	N/A	A-IBM-RATI-030719/231
rational_doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-	N/A	A-IBM-RATI-030719/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Force ID: 157383. **CVE ID : CVE-2019-4083**		
Information Exposure	27-06-2019	4	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384. **CVE ID : CVE-2019-4084**	N/A	A-IBM-RATI-030719/233
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159647. **CVE ID : CVE-2019-4249**	N/A	A-IBM-RATI-030719/234
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159648. **CVE ID : CVE-2019-4250**	N/A	A-IBM-RATI-030719/235
Improper Limitation	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0	N/A	A-IBM-RATI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883. **CVE ID : CVE-2019-4252**		030719/236
rational_engineering_lifecycle_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157383. **CVE ID : CVE-2019-4083**	N/A	A-IBM-RATI-030719/237
Information Exposure	27-06-2019	4	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384. **CVE ID : CVE-2019-4084**	N/A	A-IBM-RATI-030719/238
Improper Neutralization of Input During Web Page	27-06-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code	N/A	A-IBM-RATI-030719/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159647. **CVE ID : CVE-2019-4249**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159648. **CVE ID : CVE-2019-4250**	N/A	A-IBM-RATI-030719/240
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883. **CVE ID : CVE-2019-4252**	N/A	A-IBM-RATI-030719/241
rational_quality_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	N/A	A-IBM-RATI-030719/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157383. **CVE ID : CVE-2019-4083**		
Information Exposure	27-06-2019	4	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384. **CVE ID : CVE-2019-4084**	N/A	A-IBM-RATI-030719/243
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159647. **CVE ID : CVE-2019-4249**	N/A	A-IBM-RATI-030719/244
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159648.	N/A	A-IBM-RATI-030719/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4250		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883. **CVE ID : CVE-2019-4252**	N/A	A-IBM-RATI-030719/246
rational_rhapsody_design_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157383. **CVE ID : CVE-2019-4083**	N/A	A-IBM-RATI-030719/247
Information Exposure	27-06-2019	4	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384. **CVE ID : CVE-2019-4084**	N/A	A-IBM-RATI-030719/248
Improper Neutralization of	27-06-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to	N/A	A-IBM-RATI-030719/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159647. **CVE ID : CVE-2019-4249**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159648. **CVE ID : CVE-2019-4250**	N/A	A-IBM-RATI-030719/250
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883. **CVE ID : CVE-2019-4252**	N/A	A-IBM-RATI-030719/251
rational_software_architect_design_manager					
Improper Neutralization of Input During	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This	N/A	A-IBM-RATI-030719/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157383. **CVE ID : CVE-2019-4083**		
Information Exposure	27-06-2019	4	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384. **CVE ID : CVE-2019-4084**	N/A	A-IBM-RATI-030719/253
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159647. **CVE ID : CVE-2019-4249**	N/A	A-IBM-RATI-030719/254
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially	N/A	A-IBM-RATI-030719/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to credentials disclosure within a trusted session. IBM X-Force ID: 159648. **CVE ID : CVE-2019-4250**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883. **CVE ID : CVE-2019-4252**	N/A	A-IBM-RATI-030719/256
rational_team_concert					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157383. **CVE ID : CVE-2019-4083**	N/A	A-IBM-RATI-030719/257
Information Exposure	27-06-2019	4	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384.	N/A	A-IBM-RATI-030719/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4084		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159647. **CVE ID : CVE-2019-4249**	N/A	A-IBM-RATI-030719/259
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159648. **CVE ID : CVE-2019-4250**	N/A	A-IBM-RATI-030719/260
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883. **CVE ID : CVE-2019-4252**	N/A	A-IBM-RATI-030719/261
tivoli_netcool/impact					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	17-06-2019	7.7	IBM Tivoli Netcool/Impact 7.1.0 allows for remote execution of command by low privileged User. Remote code execution allow to execute arbitrary code on system which lead to take control over the system. IBM X-Force ID: 158094. **CVE ID : CVE-2019-4103**	https://www.ibm.com/support/docview.wss?uid=ibm10887523	A-IBM-TIVO-030719/262
security_access_manager					
N/A	25-06-2019	6.5	IBM Security Access Manager 9.0.1 through 9.0.6 is affected by a security vulnerability that could allow authenticated users to impersonate other users. IBM X-Force ID: 158331. **CVE ID : CVE-2019-4135**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/263
Information Exposure	25-06-2019	3.6	IBM Security Access Manager 9.0.1 through 9.0.6 could reveal highly sensitive in specialized conditions to a local user which could be used in further attacks against the system. IBM X-Force ID: 158400. **CVE ID : CVE-2019-4145**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/264
Improper Certificate Validation	25-06-2019	4.3	IBM Security Access Manager 9.0.1 through 9.0.6 does not validate, or incorrectly validates, a certificate which could allow an attacker to spoof a trusted entity by using a man-in-the-middle (MITM) attack. IBM X-Force ID: 158510. **CVE ID : CVE-2019-4150**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/265
Inadequate Encryption Strength	25-06-2019	4.3	IBM Security Access Manager 9.0.1 through 9.0.6 uses weaker than expected cryptographic algorithms that could allow an	https://www.ibm.com/support/docvi	A-IBM-SECU-030719/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to decrypt highly sensitive information. IBM X-Force ID: 158512. **CVE ID : CVE-2019-4151**	ew.wss?uid=ibm10888379	
Session Fixation	25-06-2019	3.6	IBM Security Access Manager 9.0.1 through 9.0.6 does not invalidate session tokens in a timely manner. The lack of proper session expiration may allow attackers with local access to login into a closed browser session. IBM X-Force ID: 158515. **CVE ID : CVE-2019-4152**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/267
URL Redirection to Untrusted Site ('Open Redirect')	25-06-2019	3.5	IBM Security Access Manager 9.0.1 through 9.0.6 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 158517. **CVE ID : CVE-2019-4153**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/268
Information Exposure	25-06-2019	4.3	IBM Security Access Manager 9.0.1 through 9.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158572. **CVE ID : CVE-2019-4156**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2019	4.3	IBM Security Access Manager 9.0.1 through 9.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158573. **CVE ID : CVE-2019-4157**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/270
N/A	25-06-2019	5.5	IBM Security Access Manager 9.0.1 through 9.0.6 does not prove that a user's identity is correct which can lead to the exposure of resources or functionality to unintended actors. IBM X-Force ID: 158574. **CVE ID : CVE-2019-4158**	https://www.ibm.com/support/docview.wss?uid=ibm10888379	A-IBM-SECU-030719/271
cognos_controller					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-06-2019	3.5	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158332. **CVE ID : CVE-2019-4136**	N/A	A-IBM-COGN-030719/272
Information Exposure	17-06-2019	4	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to obtain sensitive information, caused by a flaw in the HTTP OPTIONS method, aka Optionsbleed. By sending an	N/A	A-IBM-COGN-030719/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OPTIONS HTTP request, a remote attacker could exploit this vulnerability to read secret data from process memory and obtain sensitive information. IBM X-Force ID: 158878. **CVE ID : CVE-2019-4173**		
Information Exposure	17-06-2019	2.1	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158879. **CVE ID : CVE-2019-4174**	N/A	A-IBM-COGN-030719/274
Improper Access Control	17-06-2019	5	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to bypass security restrictions, caused by an error related to insecure HTTP Methods. An attacker could exploit this vulnerability to gain access to the system. IBM X-Force ID: 158881. **CVE ID : CVE-2019-4176**	N/A	A-IBM-COGN-030719/275
Information Exposure	17-06-2019	2.1	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158882. **CVE ID : CVE-2019-4177**	N/A	A-IBM-COGN-030719/276
pureapplication_system					
Improper Neutralization of Special Elements used in an	26-06-2019	6.5	IBM PureApplication System 2.2.3.0 through 2.2.5.3 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to	https://www-01.ibm.com/support/docview.wss?uid=	A-IBM-PURE-030719/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			view, add, modify or delete information in the back-end database. IBM X-Force ID: 159240. **CVE ID : CVE-2019-4224**	ibm1088 5602	
Informatio n Exposure Through Log Files	26-06-2019	2.1	IBM PureApplication System 2.2.3.0 through 2.2.5.3 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 159242. **CVE ID : CVE-2019-4225**	https://w ww-01.ibm.co m/suppor t/docview .wss?uid= ibm1088 5602	A-IBM-PURE-030719/278
Improper Access Control	26-06-2019	4	IBM PureApplication System 2.2.3.0 through 2.2.5.3 weakness in the implementation of locking feature in pattern editor. An attacker by intercepting the subsequent requests can bypass business logic to modify the pattern to unlocked state. IBM X-Force ID: 159416. **CVE ID : CVE-2019-4234**	https://w ww-01.ibm.co m/suppor t/docview .wss?uid= ibm1088 5602	A-IBM-PURE-030719/279
Informatio n Exposure	26-06-2019	5	IBM PureApplication System 2.2.3.0 through 2.2.5.3 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 159417. **CVE ID : CVE-2019-4235**	https://w ww-01.ibm.co m/suppor t/docview .wss?uid= ibm1088 5602	A-IBM-PURE-030719/280
Improper Access Control	26-06-2019	4.6	IBM PureApplication System 2.2.3.0 through 2.2.5.3 could allow an authenticated user with local access to bypass authentication and obtain administrative access. IBM X-Force ID: 159467.	https://w ww-01.ibm.co m/suppor t/docview .wss?uid= ibm1088	A-IBM-PURE-030719/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4241	5602	
api_connect					
Information Exposure	25-06-2019	5	IBM API Connect 5.0.0.0 through 5.0.8.6 could allow an unauthorized user to obtain sensitive information about the system users using specially crafted HTTP requests. IBM X-Force ID: 162162. **CVE ID : CVE-2019-4382**	https://www.ibm.com/support/docview.wss?uid=ibm10886747	A-IBM-API_-030719/282
sterling_b2b_integrator					
Information Exposure	25-06-2019	4	IBM Sterling B2B Integrator 6.0.0.0 and 6.0.0.1 reveals sensitive information from a stack trace that could be used in further attacks against the system. IBM X-Force ID: 162803. **CVE ID : CVE-2019-4377**	https://www.ibm.com/support/docview.wss?uid=ibm10887853	A-IBM-STER-030719/283
control_desk					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-CONT-030719/284
Improper Neutralization of Special Elements in Output Used by a Downstrea	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-CONT-030719/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
m Componen t ('Injection')					
maximo_asset_management					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-MAXI-030719/286
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-MAXI-030719/287
maximo_for_aviation					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-MAXI-030719/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-MAXI-030719/289
maximo_for_life_sciences					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-MAXI-030719/290
Improper Neutralization of Special Elements in Output Used by a Downstream Component	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-MAXI-030719/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')					
maximo_for_nuclear_power					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-MAXI-030719/292
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-MAXI-030719/293
maximo_for_oil_and_gas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-MAXI-030719/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-MAXI-030719/295
maximo_for_transportation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-MAXI-030719/296
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-MAXI-030719/297
maximo_for_utilities					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-MAXI-030719/298
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-MAXI-030719/299
smartcloud_control_desk					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-SMAR-030719/300
Improper Neutralization of	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote	https://www.ibm.com/supp	A-IBM-SMAR-030719/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	ort/docview.wss?uid=ibm10887557	
tivoli_integration_composer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949. **CVE ID : CVE-2019-4303**	https://www.ibm.com/support/docview.wss?uid=ibm10887563	A-IBM-TIVO-030719/302
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680. **CVE ID : CVE-2019-4364**	https://www.ibm.com/support/docview.wss?uid=ibm10887557	A-IBM-TIVO-030719/303
cloud_private					
Cross-Site Request Forgery	18-06-2019	6.8	IBM Cloud Private 2.1.0, 3.1.0, 3.1.1, and 3.1.2 is vulnerable to cross-site request forgery which	https://www.ibm.com/supp	A-IBM-CLOU-030719/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 158338. **CVE ID : CVE-2019-4142**	ort/docview.wss?uid=ibm10885434	
campaign					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-06-2019	4	IBM Campaign 9.1.2 and 10.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 162172. **CVE ID : CVE-2019-4384**	https://www.ibm.com/support/docview.wss?uid=ibm10887817	A-IBM-CAMP-030719/305
spectrum_protect_plus					
Information Exposure	19-06-2019	2.1	IBM Spectrum Protect Plus 10.1.2 may display the vSnap CIFS password in the IBM Spectrum Protect Plus Joblog. This can result in an attacker gaining access to sensitive information as well as vSnap. IBM X-Force ID: 162173. **CVE ID : CVE-2019-4385**	N/A	A-IBM-SPEC-030719/306
I-doit					
i-doit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2019	4.3	An XSS issue was discovered in i-doit Open 1.12 via the src/tools/php/qr/qr.php url parameter. **CVE ID : CVE-2019-6965**	N/A	A-I-D-I-DO-030719/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Imagemagick					
imagemagick					
NULL Pointer Dereference	26-06-2019	4.3	A NULL pointer dereference in the function ReadPANGOImage in coders/pango.c and the function ReadVIDImage in coders/vid.c in ImageMagick 7.0.8-34 allows remote attackers to cause a denial of service via a crafted image. **CVE ID : CVE-2019-12974**	N/A	A-IMA-IMAG-030719/308
N/A	26-06-2019	4.3	ImageMagick 7.0.8-34 has a memory leak vulnerability in the WriteDPXImage function in coders/dpx.c. **CVE ID : CVE-2019-12975**	N/A	A-IMA-IMAG-030719/309
N/A	26-06-2019	4.3	ImageMagick 7.0.8-34 has a memory leak in the ReadPCLImage function in coders/pcl.c. **CVE ID : CVE-2019-12976**	N/A	A-IMA-IMAG-030719/310
Improper Initialization	26-06-2019	6.8	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the WriteJP2Image function in coders/jp2.c. **CVE ID : CVE-2019-12977**	N/A	A-IMA-IMAG-030719/311
Improper Initialization	26-06-2019	6.8	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the ReadPANGOImage function in coders/pango.c. **CVE ID : CVE-2019-12978**	N/A	A-IMA-IMAG-030719/312
Improper Initialization	26-06-2019	6.8	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the SyncImageSettings function in	N/A	A-IMA-IMAG-030719/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MagickCore/image.c. This is related to AcquireImage in magick/image.c. **CVE ID : CVE-2019-12979**		
Kcodes					
netusb.ko					
Information Exposure	17-06-2019	6.4	An exploitable arbitrary memory read vulnerability exists in the KCodes NetUSB.ko kernel module which enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. A specially crafted index value can cause an invalid memory read, resulting in a denial of service or remote information disclosure. An unauthenticated attacker can send a crafted packet on the local network to trigger this vulnerability. **CVE ID : CVE-2019-5016**	N/A	A-KCO-NETU-030719/314
Information Exposure	17-06-2019	5	An exploitable information disclosure vulnerability exists in the KCodes NetUSB.ko kernel module that enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. An unauthenticated, remote attacker can craft and send a packet containing an opcode that will trigger the kernel module to return several addresses. One of which can be used to calculate the dynamic base address of the	N/A	A-KCO-NETU-030719/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			module for further exploitation. **CVE ID : CVE-2019-5017**		
Lenovo					
system_update					
Improper Resource Shutdown or Release	26-06-2019	5	A denial of service vulnerability was reported in Lenovo System Update before version 5.07.0084 that could allow log files to be written to non-standard locations. **CVE ID : CVE-2019-6163**	N/A	A-LEN-SYST-030719/316
Livezilla					
livezilla					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-06-2019	7.5	LiveZilla Server before 8.0.1.1 is vulnerable to SQL Injection in server.php via the p_ext_rse parameter. **CVE ID : CVE-2019-12939**	N/A	A-LIV-LIVE-030719/317
Uncontrolled Resource Consumption	24-06-2019	7.1	LiveZilla Server before 8.0.1.1 is vulnerable to Denial Of Service (memory consumption) in knowledgebase.php via a large integer value of the depth parameter. **CVE ID : CVE-2019-12940**	N/A	A-LIV-LIVE-030719/318
Improper Neutralization of Special Elements used in an SQL Command	25-06-2019	7.5	LiveZilla Server before 8.0.1.1 is vulnerable to SQL Injection in functions.internal.build.inc.php via the parameter p_dt_s_d. **CVE ID : CVE-2019-12960**	N/A	A-LIV-LIVE-030719/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-06-2019	6.8	LiveZilla Server before 8.0.1.1 is vulnerable to CSV Injection in the Export Function. **CVE ID : CVE-2019-12961**	N/A	A-LIV-LIVE-030719/320
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2019	4.3	LiveZilla Server before 8.0.1.1 is vulnerable to XSS in mobile/index.php via the Accept-Language HTTP header. **CVE ID : CVE-2019-12962**	N/A	A-LIV-LIVE-030719/321
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2019	4.3	LiveZilla Server before 8.0.1.1 is vulnerable to XSS in the chat.php Create Ticket Action. **CVE ID : CVE-2019-12963**	N/A	A-LIV-LIVE-030719/322
Improper Neutralization of Input During Web Page Generation	25-06-2019	4.3	LiveZilla Server before 8.0.1.1 is vulnerable to XSS in the ticket.php Subject. **CVE ID : CVE-2019-12964**	N/A	A-LIV-LIVE-030719/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
londontrustmedia					
private_internet_access					
N/A	21-06-2019	7.2	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client 1.0.2 (build 02363) for Windows could allow an authenticated, local attacker to run arbitrary code with elevated privileges. On startup, the PIA Windows service (pia-service.exe) loads the OpenSSL library from %PROGRAMFILES%\Private Internet Access\libeay32.dll. This library attempts to load the C:\etc\ssl\openssl.cnf configuration file which does not exist. By default on Windows systems, authenticated users can create directories under C:\. A low privileged user can create a C:\etc\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine library resulting in arbitrary code execution as SYSTEM when the service starts. **CVE ID : CVE-2019-12572**	N/A	A-LON-PRIV-030719/324
Microfocus					
fortify_software_security_center					
Improper Neutralization of Input During Web Page Generation	19-06-2019	3.5	Cross-Site Scripting vulnerability in Micro Focus Fortify Software Security Center Server, versions 17.2, 18.1, 18.2, has been identified in Micro Focus Software Security Center. The vulnerability could be exploited	N/A	A-MIC-FORT-030719/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			to execute JavaScript code in user?s browser. The vulnerability could be exploited to execute JavaScript code in user?s browser. **CVE ID : CVE-2019-11649**		
Misp					
misp					
Deserialization of Untrusted Data	17-06-2019	6.5	app/Model/Server.php in MISP 2.4.109 allows remote command execution by a super administrator because the PHP file_exists function is used with user-controlled entries, and phar:// URLs trigger deserialization. **CVE ID : CVE-2019-12868**	N/A	A-MIS-MISP-030719/326
Moodle					
moodle					
URL Redirection to Untrusted Site ('Open Redirect')	26-06-2019	5.8	A flaw was found in Moodle before 3.7, 3.6.4, 3.5.6, 3.4.9 and 3.1.18. The form to upload cohorts contained a redirect field, which was not restricted to internal URLs. **CVE ID : CVE-2019-10133**	https://moodle.org/mod/forum/discuss.php?d=386523	A-MOO-MOOD-030719/327
Improper Input Validation	26-06-2019	4.3	A flaw was found in Moodle before 3.7, 3.6.4, 3.5.6, 3.4.9 and 3.1.18. The size of users' private file uploads via email were not correctly checked, so their quota allowance could be exceeded. **CVE ID : CVE-2019-10134**	https://moodle.org/mod/forum/discuss.php?d=386524	A-MOO-MOOD-030719/328
Improper Access Control	26-06-2019	5	A flaw was found in Moodle before versions 3.7, 3.6.4. A web service fetching messages was not restricted to the current	https://moodle.org/mod/forum/discu	A-MOO-MOOD-030719/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user's conversations. **CVE ID : CVE-2019-10154**	ss.php?d=386521	
Netgate					
Pfsense					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2019	4.3	In pfSense 2.4.4-p2 and 2.4.4-p3, if it is possible to trick an authenticated administrator into clicking on a button on a phishing page, an attacker can leverage XSS to upload arbitrary executable code, via diag_command.php and rrd_fetch_json.php (timePeriod parameter), to a server. Then, the remote attacker can run any command with root privileges on that server. **CVE ID : CVE-2019-12949**	N/A	A-NET-PFSE-030719/330
Netiq					
self_service_password_reset					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2019	4.3	A potential XSS exists in Self Service Password Reset, in Micro Focus NetIQ Software all versions prior to version 4.4. The vulnerability could be exploited to enable an XSS attack. **CVE ID : CVE-2019-11647**	https://www.netiq.com/documentation/self-service-password-reset-44/release-notes-sspr-44-p2/data/release-notes-sspr-44-p2.html	A-NET-SELF-030719/331
Information Exposure	24-06-2019	5	An information leakage exists in Micro Focus NetIQ Self Service	https://www.netiq.	A-NET-SELF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Password Reset Software all versions prior to version 4.4. The vulnerability could be exploited to expose sensitive information. **CVE ID : CVE-2019-11648**	com/documentation/self-service-password-reset-44/release-notes-sspr-44-p2/data/release-notes-sspr-44-p2.html	030719/332
onapp					
onapp					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-06-2019	8.5	OnApp before 5.0.0-88, 5.5.0-93, and 6.0.0-196 allows an attacker to run arbitrary commands with root privileges on servers managed by OnApp for XEN/KVM hypervisors. To exploit the vulnerability an attacker has to have control of a single server on a given cloud (e.g. by renting one). From the source server, the attacker can craft any command and trigger the OnApp platform to execute that command with root privileges on a target server. **CVE ID : CVE-2019-12491**	N/A	A-ONA-ONAP-030719/333
openfind					
mail2000					
Improper Neutralization of Input During Web Page	19-06-2019	4.3	An issue was discovered in Openfind Mail2000 v6 Webmail. XSS can occur via an '<object data="data:text/html' substring in an e-mail message (The vendor subsequently patched this).	N/A	A-OPE-MAIL-030719/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2019-9763**		
Openjpeg					
openjpeg					
Uncontrolled Resource Consumption	26-06-2019	4.3	In OpenJPEG 2.3.1, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. This issue is similar to CVE-2018-6616. **CVE ID : CVE-2019-12973**	N/A	A-OPE-OPEN-030719/335
Open-xchange					
open-xchange_appsuite					
Improper Access Control	17-06-2019	7.5	OX App Suite 7.10.0 and earlier has Incorrect Access Control. **CVE ID : CVE-2019-7158**	N/A	A-OPE-OPEN-030719/336
Information Exposure	18-06-2019	5	OX App Suite 7.10.1 and earlier allows Information Exposure. **CVE ID : CVE-2019-7159**	N/A	A-OPE-OPEN-030719/337
Oracle					
weblogic_server					
Improper Access Control	19-06-2019	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in	N/A	A-ORA-WEBL-030719/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2729**		
Otrs					
otrs					
Information Exposure	17-06-2019	5	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.8, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. In the customer or external frontend, personal information of agents (e.g., Name and mail address) can be disclosed in external notes. **CVE ID : CVE-2019-12497**	https://lists.debian.org/debian-lts-announce/2019/06/msg00004.html	A-OTR-OTRS-030719/339
Phoenixcontact					
automationworx_software_suite					
Out-of-bounds Read	24-06-2019	6.8	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to an Out-Of-Bounds Read, Information Disclosure, and remote code execution. The attacker needs to get access to an original PC Worx or Config+ project file to be able to manipulate it. After manipulation, the attacker needs to exchange the original file with the manipulated one on the	N/A	A-PHO-AUTO-030719/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application programming workstation. **CVE ID : CVE-2019-12869**		
Access of Uninitialized Pointer	24-06-2019	6.8	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to an Uninitialized Pointer and remote code execution. The attacker needs to get access to an original PC Worx or Config+ project file to be able to manipulate it. After manipulation, the attacker needs to exchange the original file with the manipulated one on the application programming workstation. **CVE ID : CVE-2019-12870**	N/A	A-PHO-AUTO-030719/341
Use After Free	24-06-2019	6.8	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to a Use-After-Free and remote code execution. The attacker needs to get access to an original PC Worx or Config+ project file to be able to manipulate it. After manipulation, the attacker needs to exchange the original file with the manipulated one on the application programming workstation. **CVE ID : CVE-2019-12871**	N/A	A-PHO-AUTO-030719/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
PHP					
php					
Improper Input Validation	18-06-2019	5	When using gdImageCreateFromXbm() function of PHP gd extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code. **CVE ID : CVE-2019-11038**	https://bugs.php.net/bug.php?id=77973	A-PHP-PHP-030719/343
Out-of-bounds Read	18-06-2019	6.4	Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash. **CVE ID : CVE-2019-11039**	https://bugs.php.net/bug.php?id=78069	A-PHP-PHP-030719/344
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2019	6.4	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash. **CVE ID : CVE-2019-11040**	https://bugs.php.net/bug.php?id=77988	A-PHP-PHP-030719/345
pivotal_software					
cloud_foundry_uaa-release					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weak Password Recovery Mechanism for Forgotten Password	19-06-2019	4.3	Cloud Foundry UAA, versions prior to 73.0.0, falls back to appending ?unknown.org? to a user's email address when one is not provided and the user name does not contain an @ character. This domain is held by a private company, which leads to attack vectors including password recovery emails sent to a potentially fraudulent address. This would allow the attacker to gain complete control of the user's account. **CVE ID : CVE-2019-3787**	https://www.cloudfoundry.org/blog/cve-2019-3787	A-PIV-CLOU-030719/346
spring_security					
N/A	26-06-2019	7.5	Spring Security, versions 4.2.x up to 4.2.12, and older unsupported versions support plain text passwords using PlaintextPasswordEncoder. If an application using an affected version of Spring Security is leveraging PlaintextPasswordEncoder and a user has a null encoded password, a malicious user (or attacker) can authenticate using a password of "null". **CVE ID : CVE-2019-11272**	https://pivotal.io/security/cve-2019-11272	A-PIV-SPRI-030719/347
Polycom					
better_together_over_ethernet_connector					
Improper Authentication	24-06-2019	3.3	VVX products using UCS software version 5.9.2 and earlier with Better Together over Ethernet Connector (BToE) application version 3.9.1 and earlier provides insufficient authentication between the BToE application	https://support.polycom.com/content/dam/polycom-support/g	A-POL-BETT-030719/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and the BToE component, resulting in leakage of sensitive information. **CVE ID : CVE-2019-10689**	lobal/documentation/insufficient-authentication-leakage-vvx-products.pdf	
unified_communications_software					
Improper Authentication	24-06-2019	3.3	VVX products using UCS software version 5.9.2 and earlier with Better Together over Ethernet Connector (BToE) application version 3.9.1 and earlier provides insufficient authentication between the BToE application and the BToE component, resulting in leakage of sensitive information. **CVE ID : CVE-2019-10689**	https://support.polycom.com/content/dam/polycom-support/global/documentation/insufficient-authentication-leakage-vvx-products.pdf	A-POL-UNIF-030719/349
Postgresql					
postgresql					
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2019	9	PostgreSQL versions 10.x before 10.9 and versions 11.x before 11.4 are vulnerable to a stack-based buffer overflow. Any authenticated user can overflow a stack-based buffer by changing the user's own password to a purpose-crafted value. This often suffices to execute arbitrary code as the PostgreSQL operating	N/A	A-POS-POST-030719/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system account. **CVE ID : CVE-2019-10164**		
Pulsesecure					
pulse_secure_virtual_application_delivery_controller					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-PUL-PULS-030719/351
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-PUL-PULS-030719/352
Uncontrolled Resource Consumpti	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment	https://www.synology.com/security/	A-PUL-PULS-030719/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	advisory/Synology_SA_19_28	
pulse_policy_secure					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-PUL-PULS-030719/354
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182,	https://www.synology.com/security/advisory/Synology_SA_19_28	A-PUL-PULS-030719/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-PUL-PULS-030719/356
pulse_connect_secure					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-PUL-PULS-030719/357
Uncontroll	18-06-2019	5	Jonathan Looney discovered that	https://w	A-PUL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ed Resource Consumption			the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	ww.synology.com/security/advisory/Synology_SA_19_28	PULS-030719/358
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-PUL-PULS-030719/359
Pydio					
cells					
N/A	19-06-2019	6.5	Pydio Cells before 1.5.0 fails to neutralize '../' elements, allowing an attacker with minimum privilege to Upload files to, and Delete files/folders from, an	N/A	A-PYD-CELL-030719/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unprivileged directory, leading to Privilege escalation. **CVE ID : CVE-2019-12901**		
Information Exposure	19-06-2019	4	Pydio Cells before 1.5.0 does incomplete cleanup of a user's data upon deletion. This allows a new user, holding the same User ID as a deleted user, to restore the deleted user's data. **CVE ID : CVE-2019-12902**	N/A	A-PYD-CELL-030719/361
Information Exposure	19-06-2019	4	Pydio Cells before 1.5.0, when supplied with a Name field in an unexpected Unicode format, fails to handle this and includes the database column/table name as pert of the error message, exposing sensitive information. **CVE ID : CVE-2019-12903**	N/A	A-PYD-CELL-030719/362
Qemu					
qemu					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-06-2019	10	The QMP migrate command in QEMU version 4.0.0 and earlier is vulnerable to OS command injection, which allows the remote attacker to achieve code execution, denial of service, or information disclosure by sending a crafted QMP command to the listening server. **CVE ID : CVE-2019-12928**	N/A	A-QEM-QEMU-030719/363
Improper Neutralization of Special Elements used in an OS	24-06-2019	10	The QMP guest_exec command in QEMU 4.0.0 and earlier is prone to OS command injection, which allows the attacker to achieve code execution, denial of service, or information disclosure by sending a crafted QMP command	N/A	A-QEM-QEMU-030719/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			to the listening server. **CVE ID : CVE-2019-12929**		
quadbase					
espressreport_es					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2019	3.5	Stored XSS within Quadbase EspressReport ES (ERES) v7.0 update 7 allows remote attackers to execute malicious JavaScript and inject arbitrary source code into the target pages. The XSS payload is stored by creating a new user account, and setting the username to an XSS payload. The stored payload can then be triggered by accessing the "Set Security Levels" or "View User/Group Relationships" page. If the attacker does not currently have permission to create a new user, another vulnerability such as CSRF must be exploited first. **CVE ID : CVE-2019-9957**	N/A	A-QUA-ESPR-030719/365
Radare					
radare2					
Double Free	17-06-2019	4.3	In radare2 through 3.5.1, cmd_mount in libr/core/cmd_mount.c has a double free for the ms command. **CVE ID : CVE-2019-12865**	N/A	A-RAD-RADA-030719/366
rdkcentral					
rdkb_ccsppandm					
Improper Neutralization of Special Elements	20-06-2019	8.5	A shell injection issue in cosa_wifi_apis.c in the RDK RDKB-20181217-1 CcspWifiAgent module allows attackers with login credentials	N/A	A-RDK-RDKB-030719/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			to execute arbitrary shell commands under the CcspWifiSsp process (running as root) if the platform was compiled with the ENABLE_FEATURE_MESHWIFI macro. The attack is conducted by changing the Wi-Fi network password to include crafted escape characters. This is related to the WebUI module. **CVE ID : CVE-2019-6962**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-06-2019	6.5	A heap-based buffer overflow in cosa_dhcpv4_dml.c in the RDK RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve remote code execution by crafting a long buffer in the "Comment" field of an IP reservation form in the admin panel. This is related to the CcspCommonLibrary module. **CVE ID : CVE-2019-6963**	N/A	A-RDK-RDKB-030719/368
Out-of-bounds Read	20-06-2019	6.5	A heap-based buffer over-read in Service_SetParamStringValue in cosa_x_cisco_com_ddns_dml.c of the RDK RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve information disclosure and code execution by crafting an AJAX call responsible for DDNS configuration with an exactly 64-byte username, password, or domain, for which the buffer size is insufficient for the final '\0' character. This is related to the CcspCommonLibrary and WebUI modules.	N/A	A-RDK-RDKB-030719/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6964		
Redhat					
cloudforms_management_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	A stored cross-site scripting (XSS) vulnerability was found in the PDF export component of CloudForms, versions 5.9 and 5.10, due to user input is not properly sanitized. An attacker with least privilege to edit compute is able to execute a XSS attack against other users, which could lead to malicious code execution and extraction of the anti-CSRF token of higher privileged users. **CVE ID : CVE-2019-10177**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10177	A-RED-CLOU-030719/370
enterprise_linux_atomic_host					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-RED-ENTE-030719/371
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective	https://www.synology.com/security/advisory/Synology_	A-RED-ENTE-030719/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	SA_19_28	
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-RED-ENTE-030719/373
enterprise_mrg					
Integer Overflow or Wraparound	18-06-2019	7.8	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit	https://www.synology.com/security/advisory/Synology_SA_19_28	A-RED-ENTE-030719/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3b4929f65b0d8249f19a50245cd88ed1a2f78cff. **CVE ID : CVE-2019-11477**		
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e. **CVE ID : CVE-2019-11478**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-RED-ENTE-030719/375
Uncontrolled Resource Consumption	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363. **CVE ID : CVE-2019-11479**	https://www.synology.com/security/advisory/Synology_SA_19_28	A-RED-ENTE-030719/376
redwoodhq					
redwoodhq					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	19-06-2019	7.5	RedwoodHQ 2.5.5 does not require any authentication for database operations, which allows remote attackers to create admin users via a con.automationframework users insert_one call. **CVE ID : CVE-2019-12890**	N/A	A-RED-REDW-030719/377
Rubygems					
rubygems					
Argument Injection or Modification	17-06-2019	5	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::UserInteraction#verbose calls say without escaping, escape sequence injection is possible. **CVE ID : CVE-2019-8321**	N/A	A-RUB-RUBY-030719/378
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-06-2019	5	An issue was discovered in RubyGems 2.6 and later through 3.0.2. The gem owner command outputs the contents of the API response directly to stdout. Therefore, if the response is crafted, escape sequence injection may occur. **CVE ID : CVE-2019-8322**	N/A	A-RUB-RUBY-030719/379
Improper Neutralization of Special Elements in Output Used by a Downstream	17-06-2019	5	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Gem::GemcutterUtilities#with_response may output the API response to stdout as it is. Therefore, if the API side modifies the response, escape sequence injection may occur.	N/A	A-RUB-RUBY-030719/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			**CVE ID : CVE-2019-8323**		
Improper Input Validation	17-06-2019	6.8	An issue was discovered in RubyGems 2.6 and later through 3.0.2. A crafted gem with a multi-line name is not handled correctly. Therefore, an attacker could inject arbitrary code to the stub line of gemspec, which is eval-ed by code in ensure_loadable_spec during the preinstall check. **CVE ID : CVE-2019-8324**	N/A	A-RUB-RUBY-030719/381
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-06-2019	5	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::CommandManager#run calls alert_error without escaping, escape sequence injection is possible. (There are many ways to cause an error.) **CVE ID : CVE-2019-8325**	N/A	A-RUB-RUBY-030719/382
Samba					
samba					
NULL Pointer Dereference	19-06-2019	4	Samba 4.9.x before 4.9.9 and 4.10.x before 4.10.5 has a NULL pointer dereference, leading to Denial of Service. This is related to the AD DC DNS management server (dnsserver) RPC server process. **CVE ID : CVE-2019-12435**	https://www.synology.com/security/advisory/Synology_SA_19_27	A-SAM-SAMB-030719/383
NULL Pointer Dereference	19-06-2019	4	Samba 4.10.x before 4.10.5 has a NULL pointer dereference, leading to an AD DC LDAP server Denial of Service. This is related	https://www.synology.com/security/	A-SAM-SAMB-030719/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to an attacker using the paged search control. The attacker must have directory read access in order to attempt an exploit. **CVE ID : CVE-2019-12436**	advisory/Synology_SA_19_27	
Seeddms					
seeddms					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-06-2019	6	SeedDMS before 5.1.11 allows Remote Command Execution (RCE) because of unvalidated file upload of PHP scripts, a different vulnerability than CVE-2018-12940. **CVE ID : CVE-2019-12744**	https://sourceforge.net/p/seeddms/code/ci/master/tree/CHANGELOG	A-SEE-SEED-030719/385
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-06-2019	3.5	out/out.UsrMgr.php in SeedDMS before 5.1.11 allows Stored Cross-Site Scripting (XSS) via the name field. **CVE ID : CVE-2019-12745**	https://sourceforge.net/p/seeddms/code/ci/master/tree/CHANGELOG	A-SEE-SEED-030719/386
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-06-2019	4.3	out/out.GroupMgr.php in SeedDMS 5.1.11 has Stored XSS by making a new group with a JavaScript payload as the "GROUP" Name. **CVE ID : CVE-2019-12801**	N/A	A-SEE-SEED-030719/387
Shopware					
shopware					
Improper	23-06-2019	4.3	Shopware before 5.5.8 has XSS	N/A	A-SHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			via the Query String to the backend/Login or backend/Login/load/ URI. **CVE ID : CVE-2019-12935**		SHOP-030719/388
Symantec					
data_loss_prevention					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	DLP 15.5 MP1 and all prior versions may be susceptible to a cross-site scripting (XSS) vulnerability, a type of issue that can enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. **CVE ID : CVE-2019-9701**	N/A	A-SYM-DATA-030719/389
Tenable					
nessus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2019	4.3	Nessus versions 8.4.0 and earlier were found to contain a reflected XSS vulnerability due to improper validation of user-supplied input. An unauthenticated, remote attacker could potentially exploit this vulnerability via a specially crafted request to execute arbitrary script code in a users browser session. **CVE ID : CVE-2019-3961**	https://www.tenable.com/security/tns-2019-04	A-TEN-NESS-030719/390
twistedmatrix					
twisted					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-06-2019	5.8	In words.protocols.jabber.xmlstream in Twisted through 19.2.1, XMPP support did not verify certificates when used with TLS, allowing an attacker to MITM connections. **CVE ID : CVE-2019-12855**	N/A	A-TWI-TWIS-030719/391
ultimatemember					
ultimate_member					
Weak Password Recovery Mechanism for Forgotten Password	21-06-2019	4	An arbitrary password reset issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It is possible (due to lack of verification and correlation between the reset password key sent by mail and the user_id parameter) to reset the password of another user. One only needs to know the user_id, which is publicly available. One just has to intercept the password modification request and modify user_id. It is possible to modify the passwords for any users or admin WordPress Ultimate Members. This could lead to account compromise and privilege escalation. **CVE ID : CVE-2019-10270**	N/A	A-ULT-ULTI-030719/392
N/A	24-06-2019	4	An issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It allows unauthorized profile and cover picture modification. It is possible to modify the profile and cover picture of any user once one is connected. One can also	N/A	A-ULT-ULTI-030719/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modify the profiles and cover pictures of privileged users. To perform such a modification, one first needs to (for example) intercept an upload-picture request and modify the user_id parameter. **CVE ID : CVE-2019-10271**		
Videolan					
vlc_media_player					
Double Free	18-06-2019	7.5	An issue was discovered in zlib_decompress_extra in modules/demux/mkv/util.cpp in VideoLAN VLC media player 3.x through 3.0.7. The Matroska demuxer, while parsing a malformed MKV file type, has a double free. **CVE ID : CVE-2019-12874**	N/A	A-VID-VLC_-030719/394
Zohocorp					
manageengine_servicedesk_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_analytics_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0,	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_browser_security_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/397
manageengine_desktop_central					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine	https://w	A-ZOH-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	ww.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	MANA-030719/398
manageengine_eventlog_analyzer					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the	https://www.manageengine.com/products/desktop-central/elevation-of-	A-ZOH-MANA-030719/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	privilege-vulnerability.html	
manageengine_firewall					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0,	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_key_manager_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_mobile_device_manager_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/402
manageengine_network_configuration_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/403
manageengine_o365_manager_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute	https://www.manageengine.com/products/desktop-central/elevation-	A-ZOH-MANA-030719/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	of-privilege-vulnerability.html	
manageengine_opmanager					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2,	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_oputils					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0,	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_password_manager_pro					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
manageengine_patch_connect_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/408
manageengine_patch_manager_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated	https://www.manageengine.com/products/desktop-central/el	A-ZOH-MANA-030719/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**	evation-of-privilege-vulnerability.html	
manageengine_supportcenter_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380,	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_vulnerability_manager_plus					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
manageengine_adselfservice_plus					
Improper Authentication	17-06-2019	7.2	An authentication bypass vulnerability in the password reset functionality in Zoho ManageEngine ADSelfService Plus before 5.0.6 allows an attacker with physical access to gain a shell with SYSTEM privileges via the restricted thick client browser. The attack uses a long sequence of crafted keyboard input. **CVE ID : CVE-2019-12476**	N/A	A-ZOH-MANA-030719/412
manageengine_netflow_analyzer					
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0,	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-ZOH-MANA-030719/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus. **CVE ID : CVE-2019-12133**		
zucchetti					
hr_portal					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-06-2019	5	Zucchetti HR Portal through 2019-03-15 allows Directory Traversal. Unauthenticated users can escape outside of the restricted location (dot-dot-slash notation) to access files or directories that are elsewhere on the system. Through this vulnerability it is possible to read the application's java sources from /WEB-INF/classes/*.class **CVE ID : CVE-2019-10257**	N/A	A-ZUC-HR_P-030719/414