

## **National Critical Information Infrastructure Protection Centre** Common Vulnerabilities and Exposures(CVE) Report

16 - 30 Jun 2019

Vol. 06 No. 12

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		F	Patch	NCII	PC ID
Operating System  Actiontes											
Actiontec											
t2200h_firm	nware										
N/A	17-06-2019	An issue was discovered on Actiontec T2200H T2200H-31.128L.08 devices, as distributed by Telus. By attack a UART adapter to the UART pon the system board, an attack can use a special key sequence (Ctrl-\) to obtain a shell with privileges. After gaining root access, the attacker can moun the filesystem read-write and make permanent modification the device including bricking the device, disabling vendor management of the device, preventing automatic upgrade and permanently installing malicious code on the device.  CVE ID: CVE-2019-12789						N//	Ą	O-ACT T220- 03071	
Canonical											
ubuntu_lint	ıx										
Integer Overflow or Wraparou nd	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,				et CP	ogy sec adv Syn	ps://w z.synol z.com/ urity/ zisory/ nology_ 19_28	O-CAN UBUN 03071	-
CV Scoring S	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	.7	7-8	8-9	9-10

(CVSS)

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 3b4929f65b0d8249f19a50245cd 88ed1a2f78cff.		
			CVE ID : CVE-2019-11477		
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-CAN- UBUN- 030719/3
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.  CVE ID: CVE-2019-11479	https://w ww.synol ogy.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-
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6 6	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereferenc e			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.synol ogy.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_contex t_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_firn	nware				
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	0-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-
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

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_fire	nware				
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 usersupplied 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

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			DoS condition.		
			CVE ID : CVE-2019-1843		
Improper Authorizati on	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		O-CIS-RV11- 030719/10
Improper Authorizati on	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 Authorizati on	19-06-2019	5	A vulnerability in the web interface of Cisco RV110W, RV130W, and RV215W Routers	N/A	O-CIS-RV11- 030719/12
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish	Date	cvss	Description & CVE ID					F	Patch	NCIII	PC ID
				remote list of d to the g vulnera authori request this vul specific of the r	llow and attacked evices the guest net ability is ization of the An attacked evices.  URI on couter.  CVE-2	r to acquat are conversed to a to						
rv130w_firm	nware											
Improper Input Validation	19-06-2	2019	5	manage Cisco R Firewal Wireles Router, Wireles allow a attacke affected denial of This vu improp supplie manage attacke vulnera malicio targete exploit to reloa DoS con	erability ement in V110W Il, Cisco ess-N Mul ess-N VPN n unautl r to cause d device, of service linerabil er valida ed data in ement in r could e ability by ous HTTF d device could al ad the de ndition. : CVE-2	terface of Wireless RV130W tifunction of RV21 Wish Router nenticates a reloute (DoS) ity is duration of the westerface. Exploit to sending of requestion of the westerface. A succession the evice and	of the s-N VPN V on VPN 5W could ed, remondition a condition to user-b-based An his g ts to a essful attacked d causin	oote on.	N/A	A	0-CIS- 03071	
Improper Authorizati on	19-06-2	2019	5	manage RV110 Routers	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker						0-CIS- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Authorizati on	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 Authorizati on	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
CV Scoring So (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	5-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID						Patch	NCII	PC ID
			specific URI on the web interface of the router.								
			CVE ID : CVE-2019-1899								
rv215w_firi	nware		GVEID	· cve 2	017 10						
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 usersupplied 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	A	0-CIS- 03071		
Improper Authorizati on	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	A	0-CIS- 03071	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Authorizati on	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	0-CIS-RV21- 030719/19
Improper Authorizati on	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	0-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	0-CIS-IOS 030719/21
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

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.		
cylan					
clever_dog_	smart_camera	_panor	rama_dog-2w_firmware		
Informatio n 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
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-12919		
Use of Hard- coded Credential s	20-06-2019	10	N/A	O-CYL-CLEV- 030719/23	
clever_dog_	smart_camera	_plus_o	log-2w-v4_firmware		
Informatio n 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 Credential s	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	0-CYL-CLEV- 030719/25
Debian					
debian_linu	ıx				
Improper	17-06-2019	4.3	An issue was discovered in Open	N/A	O-DEB-
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

Weakness	Publ	ish Date	CVSS	Description & CVE ID						Patch	NCIII	PC 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- 03071	9/26
Deserializa tion of Untrusted Data	24-0	6-2019	4.3	before attacked impact block to polymo Dependence content may be	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					ps://li debian g/debi lts- nounce 019/06 sg000 html	O-DEB DEBI- 03071	
Informatio n Exposure	17-0	6-2019	5	Ticket 7.0.x th Edition Common 5.0.36. externatinform and mand disclose	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					ps://li debian g/debi lts- nounce 019/06 sg000 html	O-DEB DEBI- 03071	
Informatio n Exposure	19-0	6-2019	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					cur app adv nta 201	ps://se rity.net o.com/ visory/ p- 19062	O-DEB DEBI- 03071	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-	.7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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		
genieacces			CVE ID: CVE-2019-12014		
wip3bvaf_fi					
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	N/A	O-GOO- ANDR- 030719/32
			CVE ID : CVE-2019-1989 In		
Out-of- bounds Write	19-06-2019	9.3	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
			In addLinks of Linkify.java, there		0-G00-
N/A	19-06-2019	9.3	is a possible phishing vector due to an unusual root cause. This could lead to remote code execution or misdirection of	N/A	ANDR- 030719/34

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

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		
Informatio n 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	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android- 9Android ID: A-116665972  CVE ID: CVE-2019-2006		N/A	0-G00- ANDR- 030719/37
Integer Overflow or Wraparou nd	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 Synchroniz ation ('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	0-G00- 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	0-G00- ANDR- 030719/42
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-120084106		
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	0-G00- 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

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

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  In NFA_SendRawFrame of nfa_dm_api.cc, there is a possible out-of-bound write due to		O-GOO- ANDR- 030719/46
Out-of- bounds Write	19-06-2019	9.3	nfa_dm_api.cc, there is a possible	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	0-G00- 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	0-G00-
CV Scoring S	Scale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6 6	-7 7-8	8-9 9-10

(CVSS)

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_rs p 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
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	7-8	8-9 9-10

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					F	Patch	NCII	PC ID
			AndroidVersions: Android kernelAndroid ID: A- 116855682References: Upstream kernel								
			CVE ID	: CVE-2	019-20	25					
Linksys											
wrt1900acs	s_firmware										
N/A	17-06-2019	5	Linksys 1.0.3.18 exists f user to ui/1.0.9 tup.js.lo webser attacke passwo to set t passwo this list randon force tl guest n	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/se tup.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	A	0-LIN- WRT1 03071	-		
Linux											
linux_kerne	el										
Integer Overflow or Wraparou nd	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				ogy sec adv Syn	ps://w 7.synol 7.com/ urity/ visory/ nology_ 19_28	0-LIN- 03071	-LINU- 9/58	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			88ed1a2f78cff.		
			CVE ID : CVE-2019-11477		
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-LIN-LINU- 030719/59
			CVE ID : CVE-2019-11478		
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.  CVE ID: CVE-2019-11479	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-LIN-LINU- 030719/60
Improper			arch/powerpc/mm/mmu_contex		
Restriction of Operations	25-06-2019	6.9	t_book3s64.c in the Linux kernel before 5.1.15 for powerpc has a bug where unrelated processes	N/A	0-LIN-LINU- 030719/61

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

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 Dereferenc e	18-06-2019	4.6	i915_gem_userptr_get_pages in drivers/gpu/drm/i915/i915_ge m_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.	N/A	O-LIN-LINU- 030719/62
			CVE ID : CVE-2019-12881		
NULL Pointer Dereferenc e	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 usermode program that omits certain NFC attributes, leading to denial of service.	N/A	O-LIN-LINU- 030719/63
			CVE ID : CVE-2019-12984		
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://b ugzilla.re dhat.com /show_bu g.cgi?id=C VE-2019- 3896	O-LIN-LINU- 030719/64
Netgear					
r7900_firm	ware				
Informatio	17-06-2019	6.4	An exploitable arbitrary memory	N/A	O-NET-
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

Weakness	Publ	ish Date	cvss		Descript	ion & CVI	E ID		ı	Patch	NCII	PC 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- 03071	
r8000_firm	ware											
Informatio n Exposure	17-0	6-2019	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	O-NET R800- 03071		
Informatio n Exposure	17-0	6-2019	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	A	O-NET R800- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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_fir	mware				
Improper Neutralizat ion 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 Wraparou nd	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://w ww.synol ogy.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		
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-RED- ENTE- 030719/70
Uncontroll ed Resource Consumpti on	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 couluse 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, 5.1.13 and is fixed in commits 967c05aee439e6e5d7d805e1953a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5b4654b9fc363.  CVE ID: CVE-2019-11479	https://w ww.synol ogy.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	ww.synol	O-RED- ENTE- 030719/72
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Wraparou nd			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 88ed1a2f78cff.  CVE ID: CVE-2019-11477	security/ advisory/ Synology_ SA_19_28	
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-RED- ENTE- 030719/73
Uncontroll ed Resource Consumpti on	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://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-RED- ENTE- 030719/74
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
				3a20ef 5f3e2b	5aee439 5c433d6 f008c22 o9fc363.	6 and 214781						
				CVE ID	: CVE-2	019-11	479					
enterprise_	linux_	desktop										
Double Free	18-0	6-2019	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				ugz dha /sh g.cg	ps://b silla.re at.com ow_bu gi?id=C 2019-	O-RED ENTE- 03071		
enterprise_	linux_	server										
Double Free	18-0	6-2019	7.2	idr_ren Linux k unprivi use this escalat and a d	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				ugz dha /sh g.cg	ps://b silla.re at.com ow_bu gi?id=C ·2019-	O-RED ENTE- 03071	
enterprise_	linux_	_server_a	nus									
Double Free	18-0	6-2019	7.2	idr_ren Linux k unprivi use this escalat	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).				ugz dha /sh g.cg	ps://b cilla.re nt.com ow_bu gi?id=C -2019-	O-RED ENTE- 03071	
enterprise_	linux_	worksta	ition									
Double Free	18-0	6-2019	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://b ugzilla.re dhat.com /show_bu		0-RED ENTE- 03071	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			use this flaw for a privilege escalation or for a system crash and a denial of service (DoS).	g.cgi?id=C VE-2019- 3896	
			CVE ID : CVE-2019-3896		
virtualizatio	on				
Integer Overflow or Wraparou nd	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-RED- VIRT- 030719/79
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	O-RED- VIRT- 030719/80
Uncontroll ed Resource	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This	https://w ww.synol ogy.com/	O-RED- VIRT- 030719/81
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
Consumpti				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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.						urity/ visory/ nology_ 19_28		
enterprise_	linux			CVEID	: CVE-2	019-11	4/9					
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-0	6-2019	9	10.9 an 11.4 ar based hauthen stack-b the use purpos suffices as the F	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.					A	O-RED ENTE- 03071	
Integer Overflow or Wraparou nd	18-0	6-2019	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					ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	O-RED ENTE- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6		-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	·						Patch	NCIIF	C ID
			88ed1a	2f78cff.							
			CVE ID	: CVE-2	019-11	477					
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478  Jonathan Looney discovered that				ogy sec adv Syn	os://w c.synol c.com/ urity/ risory/ dology_ 19_28	0-RED ENTE- 03071		
Uncontroll ed Resource Consumpti on	18-06-2019	5					ogy sec adv Syn	os://w c.synol c.com/ urity/ risory/ dology_ 19_28	0-RED ENTE- 03071		
toaruos						<u> </u>					
toaruos											
Improper Restriction	23-06-2019	7.2	apps/gsudo.c in gsudo in ToaruOS through 1.10.9 has a					N/A	A	O-TOA TOAR-	-
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descripti	on & CV	E ID		P	atch	NCII	PC 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							03071	9/86
Tp-link							L				
tl-wr1043n	d_firmware										
Improper Authentica tion	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				s. n : to	N/A	Δ	0-TP 03071	TL-W- 9/87
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 bruteforce, 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	1	O-TP 03071	TL-W- 9/88
Zyxel											
uag2100_fin	mware		A . C	-1: C			ı				
Improper Neutralizat ion 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	<b>A</b>	0-ZYX UAG2- 03071	
CV Scoring S	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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://w ww.zyxel. com/supp ort/vulne rabilities- related- to-the- Free- Time- feature.sh tml	O-ZYX- UAG2- 030719/90
uag4100_fii	rmware				
Improper Neutralizat ion 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	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest		https://w ww.zyxel. com/supp ort/vulne rabilities- related- to-the- Free- Time- feature.sh tml	O-ZYX- UAG4- 030719/92
uag5100_fii	rmware				

Weakness	Publish Date	CVSS		Descripti	on & CV	E ID		F	Patch	NCIII	PC ID
Improper Neutralizat ion 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						A	0-ZYX UAG5- 03071	
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					ww con ort, rab rela to-t Fre	e- ne- ture.sh	0-ZYX UAG5- 03071	
zywall_vpn1	100_firmware										
N/A	27-06-2019	6.4	"Free T several ZyWall attacke accoun accoun to unau or Den	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				www con ort, rab rela to-t Fre	e- ne- ture.sh	O-ZYX ZYWA 03071	-
zywall_vpn3	300_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://w ww.zyxel. com/supp ort/vulne rabilities- related-		O-ZYX ZYWA 03071	-
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

Weakness	Publi	sh Date	cvss		Descript	on & CV	E ID		F	Patch	NCIII	PC ID
				to unau or Deni	t genera thorised al of Ser : CVE-2	l netwo vice.	rk acces		Fre Tin	ne- ture.sh		
usg1100_fir	mwar	e										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06	5-2019	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						A	0-ZYX- USG1- 03071	
N/A	27-06	5-2019	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						ps://w v.zyxel. n/supp /vulne ilities- ated- the- e- ne- ture.sh	0-ZYX- USG1- 03071	
usg110_firn	nware											
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') N/A		5-2019 5-2019	4.3 6.4	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  Missing Access Control in the "Free Time" component of						N/A https://w ww.zyxel.		- 9/99 -
CV Scoring So (CVSS)	cale	0-1	1-2	several 2-3	several Zyxel UAG, USG, and  2-3 3-4 4-5 5-6				con	n/supp 7-8	USG1- 8-9	9-10

Weakness	Publi	ish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
				attacke accoun accoun to unat or Deni	devices r to genera ts by dir t genera thorised ial of Ser : CVE-2	erate gu ectly aco tor. This d netwo vice.	the ıd	rab rela to-1 Fre Tin	ne- ture.sh	03071	9/100	
usg1900_fir	mwar	·e										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06	6-2019	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.						A	0-ZYX USG1- 03071	
N/A	27-06	6-2019	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						ps://w v.zyxel. n/supp /vulne ilities- ated- che- e- ne- ture.sh	0-ZYX USG1- 03071	
usg210_firn	nware	!										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06	6-2019	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						Α	0-ZYX USG2- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descripti	on & CV	E ID		F	Patch	NCII	PC 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						ps://w v.zyxel. n/supp /vulne ilities- nted- che- e- ne- ture.sh	0-ZYX USG2- 03071	
usg2200-vp	n_firmware										
Improper Neutralizat ion 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	A	0-ZYX USG2- 03071	
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					ww con ort, rab rela to-1 Fre	ne- ture.sh	0-ZYX USG2- 03071	
usg310_firn	nware										
Improper Neutralizat ion 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		0-ZYX USG3- 03071	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descripti	ion & CV	E ID		P	atch	NCII	PC ID
Generation ('Cross-site Scripting')			param	or HTML eter. • : <b>CVE-2</b>							
N/A	27-06-2019	6.4	"Free T several ZyWall attacked account account to unat	g Access Time" con I Zyxel U. I devices er to gene Its by dir It genera Ithorised	mponen AG, USG allows a erate gu ectly acc tor. This d netwo	the d	ww com ort/ rabi rela to-t Free Tim	<b>9-</b>	0-ZYX USG3- 03071		
zywall_1100	0_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						os://w .zyxel. a/supp vulne lities- ted- he- e- e- ure.sh	O-ZYX ZYWA 03071	
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						os://w .zyxel. n/supp vulne lities- ted- he- e- ure.sh	O-ZYX ZYWA 03071	
zywall_310_	firmware										
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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://w ww.zyxel. com/supp ort/vulne rabilities- related- to-the- Free- Time- feature.sh tml	0-ZYX- ZYWA- 030719/111
			Application		
Advantech					
webaccess					
Improper Restriction of Operations within the Bounds of a Memory Buffer Improper Restriction	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  Stack-based buffer overflow in Advantech WebAccess/SCADA	N/A	A-ADV- WEBA- 030719/112
of Operations within the Bounds of a Memory Buffer	18-06-2019	7.5	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 Neutralizat ion 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&p age=up URI.  CVE ID: CVE-2019-12905	N/A	A-AFI-FILE- 030719/114
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

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 akeysdir option that causes acceptance of an untrusted signing key.  CVE ID: CVE-2019-12875	https://se curity.net app.com/ advisory/ ntap- 2019062 5-0005/	A-ALP-ABUI- 030719/115
alternate-to	ools				
alternate_p	ic_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+0x00 000000000008868.  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+0x00 0000000000a9a1b.  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+0x00 0000000000b916d.  CVE ID: CVE-2019-12895	N/A	A-ALT- ALTE- 030719/118

CV Scoring Scale	0-1	1-2	2-3	3_/1	4-5	5-6	6-7	7-8	<b>8</b> -0	9-10
(CVSS)	0-1	1-2	2-3	5-4	4-5	3-0	0-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
analogic					
poste.io					
Protection Mechanis m 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					
Uncontroll ed Resource Consumpti on	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://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_29	A-APA- TOMC- 030719/120
allura					
Improper Neutralizat ion 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					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1	12	2 3	7	7	5	,	0	)	3 10

Weakness	Publish Dat	ce CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
jira		<u> </u>									
Improper Access Control	26-06-201	9 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						A	A-ATL 03071	-
bcnquark											
quarking_p	assword_m	anager									
Improper Input Validation	24-06-201	9 4.3	Manage clickjace by alloweb_ace attacked this vulsignifice	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					A	A-BCN QUAR- 03071	-
Bzip											
bzip2											
Out-of- bounds Write	19-06-201	9 7.5	in bzip of-bour many s	ecompre 2 throug nds writ selectors	th 1.0.6 l e when t	nas an o	ut-	N/A	A	A-BZI- 03071	BZIP- 9/124
Cesanta											
mongoose											
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-06-201	9 7.5	An issue was discovered in Mongoose before 6.15. The parse_mqtt() function in mg_mqtt.c has a critical heapbased buffer overflow.  CVE ID: CVE-2019-12951					N/A	Α	A-CES- MONG 03071	-
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	2-3 3-4 4-5 5-6			6	5-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cisco					
data_center	_network_mai	nager			
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
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1622		
integrated_	management_	contro	ller		
Informatio n 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 Wraparou nd)	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

4-5

5-6

6-7

8-9

9-10

7-8

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		P	atch	NCIII	PC ID
Missing Authentica tion for Critical Function	19-0	6-2019	5	configu Cisco In Control unauth to have arbitra The vul failure upload exploit crafting upload device. attacke or uplo	erability ration in ration in regrate ller (IMC enticate write a ry data t lnerabili to delete ed files. this vul- g a malic ing it to An expl at to fill to ad malic	mport und Manage C) could d, remote coess and to the file the affect out could be the file the affect out could be the file cours screen and the fil	gement allow ar te attack d upload esystem e to a rarily ker coul by by and cted d allow t lesystem	ter d d .	N/ <i>l</i>	A	A-CIS- 03071	INTE- 9/132
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-0	6-2019	2.1	CVE ID: CVE-2019-1629  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.				ng ng	N/A	A	A-CIS- 03071	INTE- 9/133
Missing Authentica tion for Critical Function	19-0	6-2019	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			ı	N/A	A	A-CIS- 03071	INTE- 9/134	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	2-3 3-4 4-5 5-6			6-	7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Neutralizat ion 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
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	7-8	8-9 9-10

Weakness	Publ	ish Date	cvss		Descript	ion & CVI	E ID		F	Patch	NCII	PC ID
('OS Command Injection')				attacker vulnerate with the and sulth the affect success attacker commands attacker	ed input and inp	exploit to authen istrator affecte crafted nmands oit could cute arbi	his ticating passwo d device input to . A I allow t itrary ee with	rd e				
prime_servi	ce_ca	talog									,	
Cross-Site Request Forgery (CSRF)	19-0	6-2019	6.8	manage Prime S could a remote cross-s attack of vulnera CSRF p the wel interfact An atta vulnera user of malicion exploit to perfet the printing.	erability ement in Service (Ilow and attacker ite requestion an affability is rotection behaved ce on an acker could allorm arbivilege lever to the intervilege lever to th	catalog Sunauther to condest forged ected sy due to it mecha manage affected ald exploy persuantace to A successiow the trary activel of the catalog affected well of the catalog activel of the catalog actively activ	of Cisco of tware of the contract of the contr	e I, F) he ent n	N/A	A	A-CIS- 03071	PRIM- 9/137
Improper Neutralizat ion of Input During Web Page Generation	19-0	6-2019	3.5	manage Prime S an auth to cond (XSS) a	erability ement in Service ( nenticate luct a cro ttack aga esed inte	terface (Catalog condition)  add, remo coss-site so	of Cisco ould all te attack scripting ser of th	ow ker	N/A	A	A-CIS- 03071	PRIM- 9/138
CV Scoring So (CVSS)	cale	0-1	1-2				6	-7	7-8	8-9	9-10	

Weakness	Publ	ish Date	cvss		Descript	ion & CV	E ID		ı	Patch	NCII	PC ID
('Cross-site Scripting')				validate by the interface exploit adding configue exploit to executive consisting inform	ability is ion of us web-bas ce. An at this vulication for the arbite arbite arbite attack of the at	eer-supped mana tacker conerability strings felds. A solow the trary scray he inter ker to accer-base	elied inp agement ould ty by to multi successf attacker ript code face or ecess	ut t ple ul r				
wide_area_a	applic	ation_se	rvices									
Missing Authentica tion for Critical Function	19-0	6-2019	5	proxy f Applica Softwa unauth to use f HTTPS due to of prox attacke vulnera malicio messag A succe the atta interne normal policie	erability feature of ation Server could the Centre proxy. The insufficity connects or could of ability by ous HTTI ge to the the cessful expected of t	f Cisco Verices (Verices (Veri	Wide Are VAAS)  n  te attack ager as a erability aenticati quests. A chis g a VECT Manage ald allow bublic would corpor	ker an y is on An	N/A	A	A-CIS- 03071	WIDE- 9/139
security_ma	nage	r										
Improper Restriction of XML External	19-0	6-2019	6.4	A vulnerability in Cisco Security Manager could allow an unauthenticated, remote attacker to access sensitive information or			ker	N/A	A	A-CIS- 03071	SECU- 9/140	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publ	ish Date	cvss		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
Entity Reference ('XXE')				conditi due to i XML en exploit sending targete referen An expl attacke local sy disclosi informa applica resourc conditi	denial of on. The simprope of this vulue of system or to retraction, or tion to coes, resure on.	vulneral or restrice on attack nerabilite ous reque on that co on XML d allow i eve file esulting i cause the consume lting in	ctions or er could by by ests to a contain entities from the he e availab	l he				
unified_con	ıputir	ıg_syster	n									
Informatio n Exposure	19-0	6-2019	4	Utilities Manage could a remote unauth user ins configu on the a vulnera protect configu could e downlo	erability s of Cisco ement Co ellow an a elattacke orized a formation dration of affected ability is cion of da exploit the oading the exploit of exploit	o Integral ontrolle authent of the gain coess to on from ata that system. due to it ata in the lie. An ata is vulned the sense om the fires.	ated r (IMC) icated, sensitive the is store The nsufficion e ettacker erability guration low the sitive le to	d ent by	N/A	A	A-CIS- 03071	UNIF- 9/141
Integer Underflow (Wrap or	19-0	6-2019	2.1	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an			nt	N/A	A	A-CIS- 03071	UNIF- 9/142	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6		-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descripti	on & CVI	ID		Pa	atch	NCII	PC ID
Wraparou nd)			cause a in a der conditi The vuincorre attacked vulnera HTTP r system the attacked overflocrash a device.	ticated, land buffer of the condition of the councer could endility by the cequest to councer to co	rvice (D affected ty is due ds check exploit the sending to the aff oit could cause a l ting in a	r, resulting oS) d device. e to ing. An his g a crafte fected d allow ouffer process n on the	ed				
Missing Authentica tion for Critical Function	19-06-2019	5	configu Cisco In Contro unauth to have arbitra The vu failure upload exploit crafting upload device. attacke or uplo	erability aration in tegrated ller (IMC enticated write acry data to delete ed files. At this vulrig a malicing it to the An exploser to fill up ad malicing exploser to fill up and malicing exploser to fill up a	mport ut d Manag d) could d, remot ecess and o the file ty is due e tempor An attac nerabilit ious file the affect ip the file	tement allow and the attack dupload esystem. The to a carily ker could by and eted allow the esystem ipts.	er l d	N/A		A-CIS- 03071	UNIF- 9/143
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- 03071	UNIF- 9/144
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10

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 Authentica tion 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
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publish Dat	e CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
			exploit to use a privileg arbitra device.	ous link. could all web briges of the ry action : CVE-2	low the owser a e user to ns on the	attacker nd the perform affecte	m				
Improper Neutralizat ion 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 usersupplied 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	A-CIS- 03071	
email_secur	rity_applian	ce						1			
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	A-CIS- 03071	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6				6	7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		P	atch	NCII	PC ID
prime_infra	structure		GZIP-co successi attacker content normall CVE ID	ful explor to byper filters to by drop	oit could ass conf hat wou the ema	l allow t igured ild il.	he				
N/A	19-06-2019	4	A vulner Domain Infrastr authent change configur to privil vulnera validatio attacker vulnera requests server.	system ucture ( icated, 1 the virtication, viege escapolity is could escaped bility by s sent to	of Cisco (PI) could remote a ual dome which could alation. due to it PI reque exploit to manipo an affe	o Prime Id allow attacker ain ould lead The mprope sts. An his ulating cted PI	to l r	N/A	A		PRIM- 9/149
meeting_sei	rver		allow the virtual of possibly CVE ID	ie attack domain v elevato : CVE-2	ker to ch configur e privile 019-19	ration ar ges.	e				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	19-06-2019	7.2	configuration Meeting authent inject ar root use to insuff during to vulnera attacker credent vulnera argume execution	ration so g Server icated, leading the cr. The version of the che executed the cLI with action of the ials counts during the services of the country of the	hell of Could a could a comma vulnerab nput valution of command in the command in	isco Illow an acker to nds as th oility is d idation a a d. An rator-lev it this ng crafte	ne lue vel	N/A	A		MEET- 9/150
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	C	-7	7-8	8-9	9-10

(CVSS)

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
				perfori	llow the n arbitra on an af	ary code	executi	on				
				CVE ID	: CVE-2	019-16	23					
Citrix												
appdna												
Improper Access Control	24-0	6-2019	7.5	1906.1 Access	AppDNA .0.472 h Control.	as Incor	rect		N/A	A	A-CIT- 03071	
Corel												
paintshop_p	pro_2(	019										
Integer Overflow or Wraparou nd	19-0	6-2019	6.8	PaintSh An inte parsing to over execute	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	A-COR PAIN- 03071	
Craftcms												
craft_cms												
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-0	6-2019	4.3		Craft CMS 3.1.30 has XSS.  CVE ID: CVE-2019-12823			thu /cr /cr mn 326 931 a26 e50	ps://gi b.com aftcms ns/co nit/64 eca59b ocea2c 516199 d41944	A-CRA CRAF- 03071		
Dell												
supportassi	ist_for	_busines	ss_pcs									
Uncontroll ed Search Path	25-0	6-2019	6.8	PC-Doctor Toolbox before 7.3 has an Uncontrolled Search Path Element.			ias	N/A	A	A-DEL SUPP- 03071		
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	2-3 3-4 4-5 5-6			6	6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID		
Element			CVE ID	: CVE-2	019-12	280							
N/A	20-06-2019	7.2	PCs ver Suppor version 3.0.1, 3 contain Manage malicio this vul system thread privileg machin	pportAs rsion 2.0 rtAssist f a 2.2, 2.2 a.0.2, 3.1, a an Imp ement V ous local lnerabili thread of handle t ges on the e. : CVE-2	and Delor Home .1, 2.2.2, 3.2, and roper Prulnerabi user car ty by inlusing a l to gain sy	ll e PCs , 2.2.3, 3 l 3.2.1 rivilege ility. A n exploit neriting eaked ystem	.0,	N/A	A	A-DEL SUPP- 03071			
supportassi	st_for_home_	pcs	0.2.12.10.12.2017.07.00										
		F3	DC Da	PC-Doctor Toolbox before 7.3 has									
Uncontroll ed Search Path Element	25-06-2019	6.8	an Uncontrolled Search Path Element.  CVE ID: CVE-2019-12280				N/A	A	A-DEL SUPP- 03071				
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	A-DEL SUPP- 03071				
avamar_dat	a_migration_	enabler	er_web_interface			I.							
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			Interface 1.0.50 and 1.0.51 are			,	N/A	A	A-DEL AVAM- 03071	-
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6			6	5-7 7-8		8-9	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which may allow a malicious us to download arbitrary files from the affected system by sending specially crafted request to the Web Interface application.	n a	
			CVE ID: CVE-2019-3737		
deltaww				·	•
devicenet_b	uilder				
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+0x000000000 17a45e.  CVE ID: CVE-2019-12898	00 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+0x00 0000000005e3. CVE ID: CVE-2019-12899	<sub>000</sub> N/A	A-DEL-DEVI- 030719/160
Dotcms					
dotcms					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-06-2019	6.5	dotCMS before 5.1.6 is vulneral 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	ole N/A	A-DOT- DOTC- 030719/161
Dotnetbloge	engine				
blogengine.	net				
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
Improper Restriction of XML External Entity Reference ('XXE')	21-06-2019	5	earlier Entity l pingba BlogEn lers/Pi	gine.NE' allows X Blind Inj ck.axd an gine.Cor ngbackH	ML Extendent of the control of the c	ernal related t 'HttpHa cs.		N/A	A	A-DOT BLOG- 03071	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-06-2019	6.5	and Rebecaus mishan /api/ugBlogEn ploadCissue eincomp 6714.	s Directory Traversal Code Execution creation is related to			N/A	A	A-DOT BLOG- 03071		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-06-2019	6.5	earlier and Re the the Manage becaus CVE-20	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	A-DOT BLOG- 03071		
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	A-DOT BLOG- 03071	
edrawsoft											
edraw_max			Ednow May 7 0 2 has Hoop								
Improper Restriction	19-06-2019	5	Edraw Max 7.9.3 has Heap Corruption starting at					N/A	A	A-EDR EDRA-	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6					6-7 7-8		8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID					ı	Patch	NCIII	PC ID
of Operations within the Bounds of a Memory Buffer			0x0000	tlpNtMa 0000000 : <b>CVE-2</b>	001a77		ey+			03071	9/166
Improper Access Control	19-06-2019	5	Access Instruction from Object! 000000	Max 7.9. Violatio tion Poi  Module! 0000000	n at the nter afte Paint::Cl 174.	er a call ear+0x0	00	N/A	A	A-EDR EDRA- 03071	
exacq											
enterprise_	system_mana	iger									
Improper Authorizati on	18-06-2019	6.9	Enterp (ESM) wherele escalat achieve impact and all runnin system impact or Linu permis inherit Author permis which account these deam alice back to system privilegements.	erability rise Syst v5.12.2 a by unaut ion can ped. This is exacq valued on a Wire any Wire any Wire any Wire allows a to modification file a bad action file a bad action to the servent of the servent	em Man applicati horized botentia vulnerat vision ES rsions o indows sue does adows So ments v at are no the root ers have low priv lify files es. An ex d and re that cou ctor pro ivileges. is not al	ager on privileg lly be oility SM v5.12 f ESM operation not erver OS with ot directo ?modify folders, vilege located decutable placed b ald conn viding A low ble to	ee.2.2 ng Ss, ry. e y ect	www ond s.co /m i/b ed- star ecia pag odu sec iles psa 01- exa on-	tes/sp alty- ges/pr act- urity/f s/cpp- a-2019- v2- acqvisi	A-EXA ENTE- 03071	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6			6	-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Wraparou nd	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-TRAF- 030719/169
Uncontroll ed Resource Consumpti on	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://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-TRAF- 030719/170

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
			and is f f070ef2 baf55f8	2, 4.14.12 fixed in c 2ac6671 3191a2e	commit 635706	6b683ft					
hig in again	a noliay man	agan	CVE ID	: CVE-2	019-11	478					
big-ip_acces	ss_policy_man	ager	Ionatha	an Loone	v discor	vered th	at				
Integer Overflow or Wraparou nd	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477  Jonathan Looney discovered that					ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071	
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478					ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071	
Uncontroll ed	18-06-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is					1	ps://w v.synol	A-F5-E 03071	
CV Scoring So (CVSS)	cale 0-1	1-2	the Linux kernel default MSS is  2-3 3-4 4-5 5-6					-7	7-8	8-9	9-10

Weakness	Publ	ish Date	cvss		Descript	ion & CV	ID		ı	Patch	NCIII	PC ID
Resource Consumpti on				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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.  CVE ID: CVE-2019-11479						v.com/ urity/ visory/ nology_ 19_28		
big-ip_adva	ncod	firowall	manao									
Integer Overflow or Wraparou nd		6-2019	7.8						ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-F 03071	
Uncontroll ed Resource Consumpti on	18-0	6-2019	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					ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-F 03071	BIG 9/175
CV Scoring S (CVSS)	cale	0-1	1-2					6	-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descript	ion & CVE ID		F	Patch	NCIII	PC ID
			service. This has stable kernel red 4.9.182, 4.14.12 and is fixed in conformal formal	eleases 4.4.182 27, 4.19.52, 5.1 commit 6357066b683	, .11,				
			CVE ID : CVE-2						
Uncontroll ed Resource Consumpti on	18-06-2019	5	Jonathan Loone the Linux kerne hard-coded to allows a remote TCP resend que more than if a lenforced. A remuse this to caus service. This has stable kernel reads and is fixed in comparison of the stable hard in comparison of the st	el default MSS in the bytes. This ele peer to fragme eues significant arger MSS were note attacker of eleases 4.4.182 eleases eleases eleases 4.4.182 eleases	is nent tly re ould , , .11,	ogy sec adv Syn	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071	
big-ip_analy	tics/								
Integer Overflow or Wraparou nd	18-06-2019	7.8	Jonathan Loone the TCP_SKB_C. >tcp_gso_segs was to an integer of Linux kernel was Selective Acknowledge (SACKs). A remuse this to caus service. This has stable kernel reduced to the stable with the stable kernel reduced to the stable with the stable kernel reduced to the stable with the stable kernel reduced to the stable kernel redu	B(skb)- ralue was subjected in the hen handling Towledgments ote attacker contains a denial of see a denial of see see 4.4.182, 4.19.52, 5.1 commit	ect CCP ould	ogy sec adv Syn	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071	
CV Scoring So	cale 0-1	1-2	2-3 3-4	4-5 5-6	6	-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11477		
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/178
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.  CVE ID: CVE-2019-11479	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/179
big-ip_appli	ication_accele	ration_	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://w ww.synol ogy.com/ security/	A-F5-BIG 030719/180
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	5-7 7-8	8-9 9-10

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 3b4929f65b0d8249f19a50245cd 88ed1a2f78cff.  CVE ID: CVE-2019-11477	advisory/ Synology_ SA_19_28	
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/181
Uncontroll ed Resource Consumpti on	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://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/182
CV Scoring So (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	5-7 7-8	8-9 9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID						
				5f3e2b	5c433d6 f008c22 o9fc363.	214781	01ee72	f5c										
					: CVE-2	019-11	479											
big-ip_appli	catio	n_securi	ty_man		an Loone						T							
Integer Overflow or Wraparou nd	18-0	6-2019	7.8	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477  Jonathan Looney discovered that the TCP retransmission queue					ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071							
				Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment														
Uncontroll ed Resource Consumpti on	18-0	6-2019	5	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478					ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071							
Uncontroll ed Resource	18-0	6-2019	5	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This							the Linux kernel default MSS is				ww	ps://w v.synol v.com/	A-F5-E 03071	
CV Scoring So	cale	0-1	1-2	2-3 3-4 4-5 5-6				6	6-7 7-8		8-9	9-10						

Weakness	Publ	ish Date	cvss	S Description & CVE ID					ı	Patch	NCIII	PC ID
Consumpti				more the enforce use this service stable I 4.9.182 and is fine 967c05 3a20ef 5f3e2b b4654I	a remote send que han if a led. A ren s to caus . This has kernel refixed in caee43965c433d6f008c22c9fc363.	eues sigrarger Manote atta e a denial s been feleases 4 27, 4.19. commits e6e5d7c 5 and 214781	nificantly SS were acker con al of ixed in 4.182, 52, 5.1.1	y uld l1,	adv Syr	urity/ visory/ nology_ 19_28		
big-ip_doma	ain na	ame syst	tem	CVE ID : CVE-2019-11479								
Integer Overflow or Wraparou nd	18-0	6-2019	7.8	the TCl >tcp_gg to an ir Linux k Selectiv (SACKs use this service stable l 4.9.182 and is f 3b4929 88ed1a CVE ID	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 88ed1a2f78cff.					ps://w v.synol v.com/ urity/ visory/ nology_ _19_28	A-F5-E 03071	
Uncontroll ed Resource Consumpti on	18-0	6-2019	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					ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ _19_28	A-F5-F 03071	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3 3-4 4-5 5-6				6	6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS		Descript		F	Patch	NCIII	PC ID		
			4.9.182 and is f f070ef2	xernel re 2, 4.14.12 ixed in c 2ac6671 3191a2e	27, 4.19. commit 635706	<b>52,</b> 5.1.1					
			CVE ID	: CVE-2	019-11	478					
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.  CVE ID: CVE-2019-11479						ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071	
big-ip_edge	_gateway										
Integer Overflow or Wraparou nd	18-06-2019	7.8	the TCl >tcp_gs to an ir Linux k Selectiv (SACKs use this service stable l 4.9.182 and is f 3b4929 88ed1a	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477						A-F5-E 03071	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6					-7	7-8	8-9	9-10

Weakness	Publis	h Date	cvss		Descript	ion & CVI	E ID		F	Patch	NCIII	PC ID
Uncontroll ed Resource Consumpti on	18-06-	-2019	5	the TCI implem in the I fragme certain Acknow sequen could uservice stable 4.9.182 and is ff f070ef2 baf55f8	nn Loone P retrans nentation Linux ken nted wh TCP Sel- vledgme ces. A re se this to This ha kernel re 2, 4.14.12 ixed in c 2ac6671 3191a2e : CVE-2	emission in tcp_ enel coul en hand ective int (SAC mote at o cause a s been f eleases 4 27, 4.19. ommit 635706	queue fragmen ld be ling K) tacker a denial ixed in .4.182, 52, 5.1.1	of	ogy sec adv Syn	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-F 03071	8IG 9/190
Uncontroll ed Resource Consumpti on	18-06-	-2019	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.  CVE ID: CVE-2019-11479					nt y uld	ogy sec adv Syn	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-BIG 030719/191	
big-ip_fraud_protection_service												
Integer Overflow or Wraparou nd	Overflow or 18-06-2019 Wraparou		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://w ww.synol ogy.com/ security/ advisory/ Synology_		A-F5-BIG 030719/192	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			(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 88ed1a2f78cff.  CVE ID: CVE-2019-11477  Jonathan Looney discovered that	SA_19_28		
Uncontroll ed Resource Consumpti on	18-06-2019	5	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/193	
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/194	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID								
			b4654l	9fc363.															
			CVE ID	: CVE-2	019-11	479													
big-ip_globa	al_traffic_man	ager																	
Integer Overflow or Wraparou nd	18-06-2019	7.8	the TCF >tcp_gs to an in Linux k Selectiv (SACKs use this service stable k 4.9.182 and is f 3b4929	an Loone P_SKB_C so_segs valeger over kernel wave Acknown of A rem so to caus and This has kernel rec and the control of the properties of the control and the control of the control of the and the control of the cont	B(skb)- ralue wa rerflow i hen han owledgm ote attac e a deni s been f eleases 4 27, 4.19. ommit	s subject in the dling TC nents cker cout al of ixed in 4.182, 52, 5.1.1	et IP Ild	ogy sec adv Syn	os://w v.synol v.com/ urity/ risory/ nology_ 19_28	A-F5-E 03071									
			CVE ID : CVE-2019-11477																
Uncontroll ed Resource Consumpti on	18-06-2019	5	the TCI implem in the I fragme certain Acknow sequen could uservice stable I 4.9.182 and is ff f070ef2	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.					ps://w v.synol v.com/ urity/ risory/ tology_ 19_28	A-F5-E 03071									
Uncontroll ed Resource Consumpti on	18-06-2019	5	the Linux kernel default MSS is hard-coded to 48 bytes. This						the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment			hard-coded to 48 bytes. This allows a remote peer to fragment			ent	ww ogy sec	ps://w v.synol v.com/ urity/ risory/	A-F5-E 03071	
CV Scoring So (CVSS)	cale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6					-7	7-8	8-9	9-10								

Weakness	Publish Date	CVSS		Descript	ion & CVI	ID		ı	Patch	NCIII	PC ID
			enforce use this service stable l 4.9.182 and is f 967c05 3a20ef 5f3e2b b4654l	han if a led. A rens to caus . This ha kernel re 2, 4.14.12 ixed in caee439 fo 5c433de fo 08c22 o 9fc363.	note atta e a denia s been f eleases 4 27, 4.19. commits e6e5d7d 5 and 214781		nology_ _19_28				
big-ip_link_	controller										
Integer Overflow or Wraparou nd	18-06-2019	7.8	the TCI >tcp_gs to an ir Linux k Selective (SACKs use this service stable k 4.9.182 and is f 3b4929 88ed1a	en Loone P_SKB_C So_segs venteger oventeger oven we Acknown So to caus This has kernel rec 2, 4.14.12 Fixed in control 2f65b0d a2f78cff.	B(skb)- value wa verflow i hen han owledgm ote attac e a denia s been f eleases 4 27, 4.19. commit 8249f19	s subject n the dling TC tents cker cout al of ixed in .4.182, 52, 5.1.1	t EP ald	ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ _19_28	A-F5-F 03071	8IG 9/198
Uncontroll ed Resource Consumpti on	18-06-2019	5	the TCI implem in the I fragme certain Acknow sequen could uservice stable I	en Loone P retrans nentation Linux ken nted wh TCP Sel wledgme ces. A re ase this t This ha kernel re 2, 4.14.12	smission in in tcp_ rnel coul en hand ective ent (SAC emote at o cause a s been f	of	ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-F 03071	BIG 9/199	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6						7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			and is fixed in commit f070ef2ac66716357066b683fb0 baf55f8191a2e.			
			CVE ID: CVE-2019-11478			
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/200	
big-ip_local	_traffic_manag	ger				
Integer Overflow or Wraparou nd	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/201	
Uncontroll ed	18-06-2019	5	Jonathan Looney discovered that the TCP retransmission queue	https://w ww.synol	A-F5-BIG 030719/202	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
Resource Consumpti on				in the I fragme certain Acknow sequen could uservice stable I 4.9.182 and is ff f070ef2 baf55f8	nentation inux ker nted whe TCP Sel wledgme ces. A rease this taxernel rease this taxernel rease the ces. A 14.14.12 ixed in ces. 2ac6671 in c	en hand ective ent (SAC mote at o cause s been f eleases 4 27, 4.19. commit 635706	ld be ling  K) tacker a denial ixed in 4.182, 52, 5.1.1	of l1,	sec adv Syr	v.com/ urity/ visory/ nology_ 19_28		
Uncontroll ed Resource Consumpti on		6-2019	5	the Lin hard-co allows TCP res more the enforce use this service stable lades and is for 967c05 3a20ef 5f3e2b b4654la	an Loone ux kerned oded to 4 a remote send que han if a led. A remote sto caus at the case of the case	el defaul 48 bytes e peer to eues sigr arger M note atta e a deni s been f eleases 4 27, 4.19. commits e6e5d7c 5 and 214781	t MSS is. This of fragme nificantly SS were acker contained in e.4.182, 52, 5.1.1	ent y uld	ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-F 03071	
big-ip_polic	y_enf	orcemen	t_mana						ı		,	
Integer Overflow or Wraparou nd	18-0	6-2019	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						ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-F5-E 03071	BIG 9/204
CV Scoring S (CVSS)	cale	0-1	1-2						-7	7-8	8-9	9-10

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 3b4929f65b0d8249f19a50245cd 88ed1a2f78cff.  CVE ID: CVE-2019-11477		
			Jonathan Looney discovered that the TCP retransmission queue		
Uncontroll ed Resource Consumpti on	18-06-2019	5	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/205
			CVE ID : CVE-2019-11478		
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-F5-BIG 030719/206

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		F	atch	NCI	IPC ID
			CVE ID	: CVE-2	019-11	479					
big-ip_weba	accelerator										
Integer Overflow or Wraparou nd	18-06-2019	7.8	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 88ed1a2f78cff.				c.synol c.com/ urity/ isory/ ology_	A-F5- 0307	BIG 19/207		
			CVE ID	: CVE-2	019-11	477					
Uncontroll ed Resource Consumpti on	18-06-2019	5	the TClimplen in the I fragme certain Acknow sequent could uservice stable 4.9.182 and is for the I for th	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.					os://w c.synol c.com/ urity/ isory/ ology_ 19_28	A-F5- 0307:	BIG 19/208
Uncontroll ed Resource Consumpti on	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						os://w s.synol s.com/ urity/ risory/ ology_	A-F5- 03072	BIG 19/209
CV Scoring S	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Fasterxml			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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.  CVE ID: CVE-2019-11479	SA_19_28	
jackson-dat	abind				
Deserializa tion 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://li sts.debian .org/debi an-lts- announce /2019/06 /msg000 19.html	A-FAS-JACK- 030719/210
Informatio n Exposure	19-06-2019	4.3	A Polymorphic Typing issue was discovered in FasterXML jacksondatabind 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://se curity.net app.com/ advisory/ ntap- 2019062 5-0006/	A-FAS-JACK- 030719/211
fusionpbx					
fusionpbx					
CV Scoring So (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Informatio n Exposure	17-06-2019	4	app/operator_panel/index_inc.ph p 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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-06-2019	4.3	XSS in app/operator_panel/index_inc.ph p 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 Neutralizat ion 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-
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID	
Neutralizat ion of Special Elements used in a Command ('Comman d Injection')			4.4.3 st injection lack of allows adminition	Module offers from the value input value authent strative comma c: CVE-2	om a corrability of the correction of the correc	nmand due to a , which rs to the host				03071	9/215
glyphandco	g										
xpdfreader											
Out-of- bounds Read	24-06-2019	6.8	read co FoFiTy fofi/Fo index r charsel exampl a crafte pdftops to use a Denial inform have un	•	riggered onvertTo C.cc who s larger ounds. I ggered b ocumen allows a pdf file ce or an ok, or po	in Type1 if en the than the t can, fo by sending t to the an attack to cause ssibly impact.	e r ng xer	N/A	A	A-GLY XPDF- 03071	
Out-of- bounds Read	24-06-2019	4.3	buffer of trigger FoFiTy fofi/Fo trying to private becaus has onl	have unspecified other impact.  CVE ID: CVE-2019-12957  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					A	A-GLY XPDF- 03071	
GNU											
binutils											
Out-of-	26-06-2019	4.3	An issu	e was di	scovere	d in the		N/A	A	A-GNU	<b>J</b> -
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6					6-7 7-8		8-9	9-10

Weakness	Publi	sh Date	cvss	Description & CVE ID					F	Patch	NCII	NCIIPC ID	
bounds Read				library distribe There i over-re becaus mishan of type trailing	File Des (aka lib) uted in (as a heap ead in _b e elf_obj adles an SHT_GR g'\0' cha	ofd), as and Bing Bing Bing Bing Bing Bing Bing Bing	utils 2.33 ouffer nt in bfd elfcode. idx secti omitting	.c h on			BINU- 03071	9/218	
Gnupg													
libgcrypt													
N/A	19-06	5-2019	4.3	implen vulnera side-ch physica to othe implen platfor langua unavail	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/ <i>I</i>	A	A-GNU LIBG- 03071	J- 9/219	
Google													
chrome													
Use After Free	27-06	5-2019	6.8	Chrom allowed potenticorrup page.	er free in e prior to d a remotially expetion via a correct co	o 74.0.3' ite attacl loit hear a craftec	729.108 ker to o l HTML		N/A	A	A-GOC CHRO- 03071		
Use After Free	27-06	5-2019	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	A-GOC CHRO- 03071		
CV Scoring S (CVSS)	cale	0-1	1-2	2-3 3-4 4-5 5-6				6-	7	7-8	8-9	9-10	

Weakness	Publish Date	cvss		Descripti	on & CV	E ID		F	Patch	NCII	PC ID
			HTML p	oage.							
			CVE ID	: CVE-2	019-58	09					
Informatio n Exposure	27-06-2019	4.3	Google 74.0.37 attacke sensitiv process HTML p	Ü	prior to allowed in poten ation for y via a c	a remot ntially com crafted	e	N/A	A	A-GOC CHRO 03071	
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  Incorrect security UI in popup						A	A-GOC CHRO 03071	
N/A	27-06-2019	4.3	blocker prior to remote navigat crafted	in Goog 75.0.37 attacker ion restr HTML p	le Chron 70.80 a to byp- rictions age.	me on iC llowed a ass via a		N/A	Α	A-GOC CHRO 03071	
ш			CVE ID	: CVE-2	019-58	40					
HP											
support_ass	sistant		IID C		0	7.50	1			ı	
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.						ps://s port.hp m/us- /docu nt/c06 8027	A-HP- 03071	SUPP- 9/225
				: CVE-2							
N/A	25-06-2019	7.2	HP Sup earlier system	d	upp	ps://s port.hp m/us-	A-HP- 03071	SUPP- .9/226			
CV Scoring S	cale	4.0	0.0					_		2.5	6.40
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publis	sh Date	cvss	Description & CVE ID					F	Patch	NCIII	PC ID
				directo	orized n ries or f nt vulne 328.	iles. Not	e: A	Ε-	me	'docu nt/c06 3027		
				CVE ID	: CVE-2	019-63	29					
IBM												
rational_col	labora	tive_lif	ecycle_	manage	ment							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06	5-2019	3.5	(IBM R Lifecyc through cross-s vulnerate embed in the V intended leading within Force I	zz Foundational (le Managh 6.0.6.1 ite scrip ability all arbitrar Veb UI to credus to credus 1573; c CVE-2	Collaborgement () is vulnating. This lows used but alternality pentials described assistants.	ative 6.0 erable to ers to cript cod ring the potentia lisclosur 1. IBM X	le illy e	N/A	A	A-IBM 03071	
Informatio n Exposure	27-06	5-2019	4	(IBM R Lifecyc through authen sensitive Application further system CVE ID	zz Found ational ( le Manag h 6.0.6.1 ticated u ve informations the attacks . IBM X-	Collabor gement ( ) could a user to o nation fo at could against Force ID <b>019-40</b>	ative 6.0 allow an btain rom CLM be used the 1: 15738	⁄I l in	N/A	A	A-IBM 03071	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	27-06	5-2019	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	A-IBM 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3 3-4 4-5 5-6					-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descript	ion & CVI	E ID		ı	Patch	NCIII	PC ID
Scripting')				a trusted D: 1596		n. IBM X	-				
						40					
				: CVE-2							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	(IBM R Lifecyc through cross-s vulnera embed in the V intended leading within Force I	IBM Rational Collaborative					A		-RATI- 9/230
			CVE ID	CVE ID : CVE-2019-4250							
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	Lifecyc through remote directo attacke crafted "dot do arbitra	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.				N/A	A		-RATI- 9/231
vational do	and novet done	wation	CVETE		017 12						
rauonai_do	ors_next_gene	ration	1D111		1					1	
Improper Neutralizat ion 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		-RATI- 9/232	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	2-3 3-4 4-5 5-6				-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Descripti	on & CVI	E ID		F	Patch	NCIII	PC ID
			Force ID	: 15738	33.						
			CVE ID:	CVE-20	019-40	83					
Informatio n Exposure	27-06-2019	4	IBM Jazz (IBM Ra Lifecycle through authenti sensitive Applicat further a system.	tional C e Manag 6.0.6.1) icated u e inform tions tha attacks a	ollaboratement ( ) could a ser to on ation from the could against force ID	ative 6.0 allow an btain com CLM be used the : 15738	⁄I l in	N/A	A	A-IBM- 03071	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159647.						A	A-IBM- 03071	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	CVE ID: CVE-2019-4249  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	A-IBM- 03071	
Improper Limitation	27-06-2019	5	IBM Rational Collaborative Lifecycle Management 6.0					N/A	Α	A-IBM	-RATI-
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publ	lish Date	cvss		Descript	ion & CV	E ID		F	Patch	NCII	PC ID
of a Pathname to a Restricted Directory ('Path Traversal')				remote directo attacke crafted "dot do arbitra X-Force	h 6.0.6.1 e attacke ries on t er could : URL rec URL rec st" seque ry files c e ID: 159	r to traveline systems as specification the systems (/) on the systems (8883.	erse em. An pecially- ntaining ./) to vie estem. IE	g ew			03071	9/236
rational_en	ginee	ring_life	cycle_m	nanager								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-0	6-2019	3.5	(IBM R Lifecyc throug cross-s vulnera embed in the V intended leading within Force I		Collabor gement () is vuln ting. This lows use y JavaSchus alter onality gentials described session 83.	ative 6.0 erable to ers to cript cod ring the potentia lisclosur n. IBM X	le illy e	N/A	A		-RATI- 9/237
Informatio n Exposure	27-0	6-2019	4	(IBM R Lifecyc throug authen sensitiv Applica further system	Force ID: 157383.  CVE ID: CVE-2019-4083  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					A		-RATI- 9/238
Improper Neutralizat ion of Input During Web Page	27-0	6-2019	3.5	IBM Ra Lifecyc throug cross-s vulnera embed		N/A	Α		-RATI- 9/239			
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publi	ish Date	CVSS		Description & CVE ID				ı	Patch	NCIII	PC ID
Generation ('Cross-site Scripting')				intende leading within	Web UI to ed functi g to credo a trusted D: 1596	onality j entials d d session	potentia lisclosur	·e				
				CVE ID	: CVE-2	019-42	49					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06	6-2019	3.5	(IBM R Lifecyc throug cross-s vulnera embed in the V intended leading within Force I	zz Found ational ( le Manag h 6.0.6.1 ite scrip ability al arbitrar Web UI t ed functi g to cred a trusted D: 1596	Collabor gement of the second	ative 6.0 erable to ers to cript cod ring the potentia lisclosur 1. IBM X	le lly e	N/A	A		-RATI- 9/240
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		6-2019	5	Lifecyc throug remote directo attacke crafted "dot do arbitra X-Force	WE ID: CVE-2019-4250  BM Rational Collaborative ifecycle Management 6.0 arough 6.0.6.1 could allow a semote attacker to traverse irectories on the system. An attacker could send a specially-rafted URL request containing dot dot" sequences (//) to view rbitrary files on the system. IBM -Force ID: 159883.  VE ID: CVE-2019-4252				N/A	A	A-IBM 03071	-RATI- 9/241
rational_qu	ality_r	managei	1									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	27-00	6-2019	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		-RATI- 9/242
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157383.		
			CVE ID: CVE-2019-4083		
Informatio n 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- 030719/243
			CVE ID : CVE-2019-4084		
Improper Neutralizat ion 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.	N/A	A-IBM-RATI- 030719/244
			IBM Jazz Foundation products		
Improper Neutralizat ion 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: 159648.	N/A	A-IBM-RATI- 030719/245
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publi	ish Date	cvss		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID			
				CVE ID	: CVE-2	019-42	50								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06	6-2019	5	through remote directo attacke crafted "dot do arbitra X-Force	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						A-IBM 03071				
rational_rha	apsody	y_design	_mana	ger											
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06	6-2019	3.5	(IBM R Lifecyc through cross-s vulnera embed in the V intended leading within Force I	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					A	A-IBM 03071				
Informatio n Exposure	27-06	6-2019	4	(IBM R Lifecyc through authen sensitiv Applica further system CVE ID	CVE ID: CVE-2019-4083  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					Α	A-IBM 03071	9/248			
Improper Neutralizat ion of	27-06	6-2019	3.5	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to					Lifecycle Management 6.0		)	N/A	A	A-IBM 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	7	7-8	8-9	9-10			

Weakness	Publish Date	CVSS		Descript	ion & CV		F	atch	NCIII	PC ID						
Input During Web Page Generation ('Cross-site Scripting')			vulnera embed in the V intende leading within	ite scrip ability al arbitrar Web UI thed functi g to credo a trusteo D: 1596	lows usery JavaSo hus alter ionality entials of	ılly re										
			CVE ID	: CVE-2	019-42	49										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	(IBM R Lifecyc through cross-s vulnerate embed in the V intended leading within Force I	zz Found ational ( le Manag h 6.0.6.1 ite scrip ability al arbitrar Web UI the d functi g to credo a trusted D: 1596 : CVE-2	Collabor gement ) is vulnting. The lows usery JavaSo hus altered and session 48.	ative 6.0 erable to ers to eript cod ring the potential disclosur 1. IBM X	le illy re	N/A	A		-RATI- 9/250					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-06-2019	5	Lifecyc through remote directo attacke crafted "dot do arbitra X-Force	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					A		-RATI- 9/251					
	tware_archite	ect_desi	ign_manager													
Improper Neutralizat ion 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						(IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) is vulnerable to			0	N/A	A		-RATI- 9/252
CV Scoring S (CVSS)	cale 0-1	1-2	2-3						7-8	8-9	9-10					

Weakness	Publish Date	cvss		Descripti	on & CV		P	atch	NCII	PC ID	
Web Page Generation ('Cross-site Scripting')			embed in the V intende leading within Force I	ability all arbitrary Web UI thed function to credon a trusted D: 15738	y JavaSo nus alter onality p entials d I session 33.	ript cod ring the potentia isclosur n. IBM X	lly e				
Informatio	27-06-2019	1	IBM Jaz (IBM R Lifecyc throug authen		ation production production at the second production at the second at th	oducts ative 6.0 allow an btain		N //		A-IBM	-RATI-
n Exposure	27-06-2019	4	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  IBM Rational Collaborative					N/A	A	03071	9/253
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-06-2019	3.5	Lifecyc through cross-s vulnera embed in the V intended leading within	CVE ID : CVE-2019-4084					Α		-RATI- 9/254
			CVE ID	: CVE-2	019-42	49					
Improper Neutralizat ion 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		-RATI- 9/255
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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.	N/A	A-IBM-RATI- 030719/256
			CVE ID : CVE-2019-4252		
rational_tea	am_concert				
Improper Neutralizat ion 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
Informatio n 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 Neutralizat ion 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 Neutralizat ion 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_netco	ol/impact				

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887523	A-IBM-TIVO- 030719/262
security_ac	cess_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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 888379	A-IBM- SECU- 030719/263
Informatio n 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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 888379	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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 888379	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://w ww.ibm.c om/supp ort/docvi	A-IBM- SECU- 030719/266

Weakness	Publish Date	· ·			NCIIPC ID
			attacker to decrypt highly sensitive information. IBM X-Force ID: 158512.	ew.wss?ui d=ibm10 888379	
			CVE ID : CVE-2019-4151		
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 888379	A-IBM- SECU- 030719/267
URL Redirectio n 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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 888379	A-IBM- SECU- 030719/268
Informatio n 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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 888379	A-IBM- SECU- 030719/269

Weakness	Publis	h Date	cvss		Descripti	ion & CVI	E ID		ı	Patch	NCIII	PC ID								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	25-06	-2019	4.3	to cross vulnera embed in the V intended leading within a Force II	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					A-IBM SECU- 03071										
N/A	25-06	-2019	5.5	9.0.1 th prove t correct exposu function actors.	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					ps://w v.ibm.c /supp /docvi .wss?ui bm10	A-IBM SECU- 03071									
cognos_con	troller																			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-06	-2019	3.5	10.2.1, is vulne scriptin allows lavaScriptin thus alt function to credit trusted 158332	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.					A	A-IBM COGN- 03071									
Informatio n 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						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			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				N/A	A	A-IBM COGN- 03071	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5 5-6 6				6-7 7-8		9-10								

Weakness	Publish Date	cvss		Descripti	on & CVI	E ID		F	Patch	NCIIPC ID
			attacke vulnera from pr sensitiv	NS HTTP er could e ability to rocess m ve inforn D: 15887	exploit to read se emory a nation. I	his cret dat and obta	a			
			CVE ID	: CVE-2	019-41	73				
Informatio n 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.					N/A	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						A	A-IBM- COGN- 030719/275
Informatio n 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.					N/A	A	A-IBM- COGN- 030719/276
pureapplica	ntion_system									
Improper Neutralizat ion 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					01.i m/s t/d	os://w /- ibm.co suppor ocview s?uid=	A-IBM- PURE- 030719/277
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	2-3 3-4 4-5 5-6			6	-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			view, add, modify or delete information in the back-end database. IBM X-Force ID: 159240.	ibm1088 5602	
			CVE ID: CVE-2019-4224		
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.	https://w ww- 01.ibm.co m/suppor t/docview .wss?uid= ibm1088 5602	A-IBM- PURE- 030719/279
			CVE ID : CVE-2019-4234		
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
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publi	sh Date	cvss		Descript	on & CV	E ID		F	Patch	NCII	PC ID
				CVE ID	: CVE-2	019-42	41		560	)2		
api_connect	Ţ											
Informatio n Exposure	25-06	5-2019	5	5.0.8.6 unauth sensitiv system crafted Force I	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						A-IBM 03071	-API 9/282
sterling_b2l	b_integ	grator										
Informatio n Exposure	25-06	5-2019	4	6.0.0.0 sensitiv stack to further system	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					ps://w v.ibm.c /supp /docvi wss?ui bm10	A-IBM STER- 03071	- 9/283
control_des	k											
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-06	5-2019	3.5	7.6 is v scriptinallows JavaScr thus alt functio to cred trusted	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.					ps://w v.ibm.c /supp /docvi wss?ui bm10 7563	A-IBM CONT- 03071	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea	19-06	5-2019	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					om ort ew. d=i	os://w v.ibm.c /supp /docvi wss?ui bm10	A-IBM CONT- 03071	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	3-4 4-5 5-6			6-7 7-8		8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
m Componen t ('Injection' )	cot managomo	nt.			
maximo_ass	set_manageme	:111	TOWN : A . W		
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887563	A-IBM- MAXI- 030719/286
T			CVE ID: CVE-2019-4303		
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887557	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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887563	A-IBM- MAXI- 030719/288
CV Scoring So (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	7-8	8-9 9-10

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		F	Patch	NCII	PC ID
Scripting')			trusted 160949	session ).	. IBM X-	Force II	D:				
			CVE ID	: CVE-2	019-43	03					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection' )	19-06-2019	8.5	7.6 is which cauthen arbirar system	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						A-IBM MAXI- 03072	
maximo_for	_life_sciences										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-06-2019	3.5	7.6 is viscripting allows JavaScripting alternation to credit trusted 160949	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.					ps://w v.ibm.c /supp /docvi wss?ui bm10	A-IBM MAXI- 03072	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t	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					om ort ew. d=i	ps://w v.ibm.c /supp /docvi wss?ui bm10 7557	A-IBM MAXI- 03072	
	<u> </u>									<u> </u>	

(CVSS)

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
('Injection'											
maximo_for	_nuclear_pow	er									
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					om ort ew d=i	ps://w v.ibm.c /supp /docvi .wss?ui bm10 7563	A-IBM MAXI- 03071	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection' )	19-06-2019	8.5	7.6 is v which of authen arbirar system	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					ps://w v.ibm.c /supp /docvi .wss?ui bm10 7557	A-IBM MAXI- 03071	
maximo_for	_oil_and_gas										
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					om ort ew d=i	ps://w z.ibm.c /supp /docvi .wss?ui bm10 7563	A-IBM MAXI- 03071	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	2-3 3-4 4-5 5-6				6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID							
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887557	A-IBM- MAXI- 030719/295							
maximo_for	_transportatio	on										
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887563	A-IBM- MAXI- 030719/296							
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887557	A-IBM- MAXI- 030719/297							
maximo_for	_utilities			maximo_for_utilities								

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887563	A-IBM- MAXI- 030719/298
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887557	A-IBM- MAXI- 030719/299
smartcloud	_control_desk				
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm10 887563	A-IBM- SMAR- 030719/300
Improper Neutralizat ion of	19-06-2019	8.5	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote	https://w ww.ibm.c om/supp	A-IBM- SMAR- 030719/301
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

Weakness	Publisl	h Date	cvss		Descript	on & CV	E ID		F	Patch	NCIII	PC ID
Special Elements in Output Used by a Downstrea m Componen t ('Injection' )				arbirar system	ticated a y comm . IBM X-I : <b>CVE-2</b>	ands on Force ID	the : 16168		ew. d=i	/docvi wss?ui bm10 7557		
tivoli_integi	ration_c	compos	er									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-06-	2019	3.5	7.6 is v scriptinallows JavaScrithus alternation to cred trusted 160949	aximo Asulnerables ag. This valuers to ript code tering the mality poentials described in the session of the control of the country poentials described in t	e to crost vulnerable embed a in the V e intend otentially isclosur . IBM X-	ss-site bility arbitrar Veb UI led y leadin re withir	y g n a	om ort ew. d=i	ps://w v.ibm.c /supp /docvi wss?ui bm10 7563	A-IBM 03071	
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			om ort ew. d=i	ps://w v.ibm.c /supp /docvi wss?ui bm10 7557	A-IBM 03071			
cloud_priva	te											
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					ibm.c	A-IBM CLOU- 03071		
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publi	sh Date	cvss		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
(CSRF)				execute unauth from a trusts.	llow an e malicic orized a user tha IBM X-F	ous and ctions to t the we orce ID:	ransmitt ebsite 158338		ew. d=i	/docvi .wss?ui bm10 5434		
campaign												
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-06	5-2019	4	could a travers system special contair (//) to the sys	mpaign llow a re e directe . An atta ly-crafte hing "dot o view an tem. IBM 2. : CVE-2	emote at ories on cker cou d URL r dot" se bitrary I X-Forc	ttacker t the uld send equest quences files on te ID:	a	om ort ew. d=i	ps://w v.ibm.c /supp /docvi .wss?ui bm10 7817	A-IBM CAMP 03071	-
spectrum_p	rotect	_plus										
Informatio n Exposure	19-06	5-2019	2.1	may dispassword password result is access well as 162173	ectrum is splay the splay the splay the sensite vSnap. Is correctly the sensite vSnap. It is correctly the sensite vSnap. It is correctly the sensite vSnap. Is correctly the sensite vSnap. It is correctly the vSnap. It is correctly the sensite vSnap. It is correctly the vSnap. It is correctly the sensite vSnap. It is corr	e vSnap e IBM Sp olog. Thi acker ga cive info BM X-Fo	CIFS Dectrum is can ining rmation orce ID:		N/A	A		-SPEC- 9/306
I-doit				<b>U</b> • • • • • • • • • • • • • • • • • • •		0 2 7 10						
i-doit												
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-06	5-2019	4.3	An XSS issue was discovered in idoit Open 1.12 via the src/tools/php/qr/qr.php url parameter.  CVE ID: CVE-2019-6965				i-	N/A	A	A-I-D- 03071	_
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	2-3 3-4 4-5 5-6				-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Imagemagick					
imagemagick					
NULL Pointer Dereferenc e	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 Initializati on	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 Initializati on	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 Initializati on	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

3-4

6-7

7-8

8-9

9-10

5-6

CV Scoring Scale

(CVSS)

0-1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Kcodes netusb.ko			MagickCore/image.c. This is related to AcquireImage in magick/image.c.  CVE ID: CVE-2019-12979		
Informatio n 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
Informatio n 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	Publ	ish Date	cvss		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
				module	e for furt	her exp	loitation					
				CVE ID	: CVE-2	019-50	17					
Lenovo												
system_upd	late											
Improper Resource Shutdown or Release	26-0	6-2019	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	A-LEN 03071	
Livezilla											•	
livezilla												
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	24-00	6-2019	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	A-LIV- 03071	-
Uncontroll ed Resource Consumpti on	24-00	6-2019	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				S	N/A	A	A-LIV- 03071	
Improper Neutralizat ion of Special Elements used in an SQL Command	25-00	6-2019	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	A-LIV- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3 3-4 4-5 5-6				6	-7	7-8	8-9	9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
('SQL Injection')												
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection' )	25-0	6-2019	6.8	vulnera Export	LiveZilla Server before 8.0.1.1 is vulnerable to CSV Injection in the Export Function.  CVE ID: CVE-2019-12961						A-LIV- 03071	LIVE- 9/320
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	25-0	6-2019	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	A-LIV- 03071	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	25-0	6-2019	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	A-LIV- 03071	LIVE- 9/322
Improper Neutralizat ion of Input During Web Page Generation	25-0	6-2019	4.3	LiveZilla Server before 8.0.1.1 is vulnerable to XSS in the ticket.php Subject.  CVE ID: CVE-2019-12964				S	N/A	A	A-LIV- 03071	LIVE- 9/323
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	2-3 3-4 4-5 5-6				-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
londontrus	tmedia				
private_inte	ernet_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					
	ware_security_	center			
Improper Neutralizat ion 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
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Descripti	on & CV	E ID		F	Patch	NCII	PC ID			
('Cross-site Scripting')			user?s l could b JavaScr browse	ute JavaS browser e exploit ipt code er. : CVE-2	. The vu ted to ex in user	lnerabili xecute ?s	ity							
Misp														
misp														
Deserializa tion of Untrusted Data	17-06-2019	6.5	2.4.109 executi adminis file_exis user-co phar:// deseria	odel/Ser allows if allows if on by a sector be strator be strator be ontrolled URLs tr lization. : CVE-2	remote of super secause ion is us entries rigger	comman the PHP sed with , and	ıd	N/A	A		-MISP- 9/326			
Moodle														
moodle														
URL Redirectio n 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.					ood /m/ um ss.p	ps://m dle.org od/for /discu ohp?d=	A-MOO MOOD 03071				
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				e	ood /m/ um ss.p	os://m lle.org od/for /discu ohp?d=	A-MOO MOOD 03071				
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				before versions 3.7, 3.6.4. A web service fetching messages was			b	ood /m	os://m lle.org od/for /discu	A-MOO MOOD 03071	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10			

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIIF	PC ID
			user's o	conversa	tions.			_	hp?d=		
			CVE ID	: CVE-2	019-10	154		386	5521		
Netgate											
Pfsense											
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	25-06-2019	4.3	if it is pauthen clicking page, a XSS to executa diag_corrd_fet parameter commathat serior	nse 2.4.4 cossible to ticated a gon a but acked able code command ach_json.peter), to a cattacked and with rver.	dminist administ atton on er can le rbitrary e, via aphp and a server r can rui	rator in a phishi verage d ePeriod . Then, t n any vileges o	to ing he	N//	A	A-NET PFSE- 03071	
Netiq											
self_service	_password_re	set									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-06-2019	4.3	Service Focus I prior to vulnera to enab	ntial XSS Passwo NetIQ So o version ability co ole an XS	rd Rese ftware a 1 4.4. Th ould be e S attack	t, in Mici ll versic e exploited	ons	www.commee. /see serr pass -rees 44// e-n sspp p2// elea not ssp	vice- sword set- 'releas otes- r-44- 'data/r	A-NET SELF- 03071	
Informatio n Exposure	24-06-2019	5		rmation Focus Ne	_		n	_	os://w v.netiq.	A-NET SELF-	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	.7	7-8	8-9	9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
				version vulnera to expo	ord Rese is prior to ability co se sensi : CVE-2	to versice ould be extincted to the contract of the contract o	on 4.4. T exploited ermation	d	me /se ser pas -res 44/e-n ssp p2/elea not ssp	vice- sword set- 'releas otes- r-44- 'data/r	03071	9/332
onapp												
onapp												
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	19-0	6-2019	8.5	and 6.0 to run a root pr manage hyperv vulnera have co a given one). Frattacke and trig to exect root pr	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	A-ONA ONAP- 03071	
openfind												
mail2000												
Improper Neutralizat ion of Input During Web Page	19-0	6-2019	4.3	An issue was discovered in Openfind Mail2000 v6 Webmail. XSS can occur via an '								

Weakness	Publish D	ate CVS	S		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
Generation ('Cross-site Scripting')				CVE ID	: CVE-2	019-97	63					
Openjpeg			<u> </u>									
openjpeg												
Uncontroll ed Resource Consumpti on	26-06-20	19 4.3		excessi opj_t1_ openjp could le to caus crafted similar	ve iteratencode_2/t1.c. Feverage e a deniate bmp file to CVE-	lemote a	ne nction o attackers nerabilit vice via a ssue is 516.	s y	N/A	A	A-OPE OPEN- 03071	
Open-xchan	ıge											
open-xchan	ge_appsu	ite										
Improper Access Control	17-06-20	7.5		has Inc	orrect A	.10.0 and .ccess Co <b>019-71</b>		•	N/A	A	A-OPE OPEN- 03071	
Informatio n Exposure	18-06-20	19 5		allows	Informa	.10.1 and tion Exp <b>019-71</b>		•	N/A	A	A-OPE OPEN- 03071	
Oracle												
weblogic_se	erver											
Improper Access Control	19-06-20	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	Α	A-ORA WEBL 03071	-
CV Scoring S (CVSS)	cale 0-	-1 1-2		2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descript	ion & CVI	E ID		F	Patch	NCIII	PC ID
			Server. (Confid Availab Vector: (CVSS:3 /S:U/C	3.0/AV:N :H/I:H/ <i>F</i>	O Base S y, Integri pacts). C I/AC:L/I A:H).	core 9.8 ity and VSS PR:N/UI					
0:			CVE ID	: CVE-2	019-27	29					
Otrs											
otrs			Ι	1.		1: 0				I	
Informatio n Exposure	17-06-2019	5	Ticket In 7.0.x the Edition Commus 5.0.36. externating and mand disclose	e was di Request rough 7 6.0.x th unity Edi In the cu al fronter ation of a ail addresed in ext : CVE-2	System .0.8, Con rough 6. tion 5.0 istomer agents (ass) can be remal no	(OTRS) nmunity .0.19, an .x throu or onal e.g., Nan oe otes.	, id gh	stsorg an- anr /20 /m	ps://li debian g/debi lts- iounce 019/06 sg000 html	A-OTR OTRS- 03071	
Phoenixcon	tact		G. = 12		V=V ==						
automation	worx_softwa	re_suite	1								
Out-of- bounds Read	24-06-2019	6.8	PHOEN through through through Worx of lead to Inform remote attacked original project maniput the attacked the original through through the original through the original thro	e was di IIX CONT h 1.86, P h 1.86, A h 1.86. A or Config an Out-C ation Dis code ex r needs I PC Won file to b alate it. A acker nee	CACT PCC Worx nd Confirmanipu + project Of-Boun sclosure ecution. to get act act or Confirmation and the confirmation with the with the confirmation with	Worx Express ig+ ilated Po it file cou ds Read , and The iccess to a infig+ inipulation icchange	Culd , an	N/A	A	A-PHO AUTO- 03071	
			manipi	ılated or	ie on the	;					

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			application programming workstation.		
			CVE ID : CVE-2019-12869		
Access of Uninitializ ed 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.	N/A	A-PHO- AUTO- 030719/341
			CVE ID : CVE-2019-12870		
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	С	Descripti	on & CV	E ID		F	Patch	NCII	PC ID
PHP											
php											
Improper Input Validation	18-06-2019	5	When us gdImage function PHP vers 7.2.x below 7. supply d function uninitial lead to d stack that previous CVE ID:	eCreatel of PHP sions 7. ow 7.2. 3.6, it is lata that to use lized va lisclosir at has b s code.	gd externance of the second se	ension in w 7.1.30 7.3.x le to use the le of This may ents of the there by	o, ne	ugs et/	ps://b s.php.n bug.ph d=779	A-PHP 03071	9-PHP- 9/343
Out-of- bounds Read	18-06-2019	6.4	Function iconv_m PHP vers 7.2.x below 7. buffer re overflow headers. informat	ime_deosions 7. ow 7.23.6 may ead due v when . This m tion dis	1.x belo 19 and ' y perfor to integ parsing ay lead closure	w 7.1.30 7.3.x m out-o ger MIME to or crash	O, f-	ugs et/	ps://b s.php.n bug.ph d=780	A-PHP 03071	9-PHP- 9/344
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2019	6.4	parsing limage, e. function below 7. and 7.3.x possible what will allocated informat	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					ps://b s.php.n bug.ph d=779	A-PHP 03071	9-PHP- 9/345
pivotal_soft	ware										
cloud_found	lry_uaa-releas	e									
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
Weak Password Recovery Mechanis m for Forgotten Password	19-0	6-2019	4.3	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					ww our g/b	ps://w v.cloudf ndry.or olog/cv 019- 37		CLOU- 9/346
spring_secu	rity											
N/A	26-0	6-2019	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".				vot ecu	ps://pi al.io/s .rity/c 2019- 272	A-PIV- 03071	_	
Polycom												
better_toge	ther_c	over_eth	ernet_c	onnecto	or							
Improper Authentica tion	24-0	6-2019	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					upp lyco m/ t/d lyco	ps://s port.po pm.co conten am/po pm- pport/g	A-POL BETT- 03071	
CV Scoring So	cale	0-1	1-2					6	-7	7-8	8-9	9-10

Weakness Publish D	ate CVSS		Descript	ion & CVI	E ID		ı	Patch	NCIII	PC ID
		resultii inform	e BToE cong in lead ation. : CVE-2	kage of s	sensitive		um n/i ien aut atio	hentic on- kage- kage- ducts.		
unified_communicati	ons_softwa	re								
Improper Authentica 24-06-20 tion	3.3	version Better Connect version insuffic betwee and the resultin inform	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					ps://s port.po om.co conten am/po om- pport/g al/doc entatio nsuffic t- hentic on- kage- coducts.		-UNIF- 9/349
Postgresql										
postgresql		Darte	COL	_:1	) l C-					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19 9	PostgreSQL versions 10.x before 10.9 and versions 11.x before 11.4 are vulnerable to a stackbased 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	A-POS POST- 03071	
CV Scoring Scale (CVSS)	-1 1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
				system	account	-						
				CVE ID	: CVE-2	019-10	164					
Pulsesecure	9											
pulse_secur	e_virt	ual_app	lication	_delive	ry_cont	roller						
Integer Overflow or Wraparou nd	18-0	6-2019	7.8	>tcp_gs to an ir Linux k Selectiv (SACKs use this service stable k 4.9.182 and is f 3b4929 88ed1a	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477  Jonathan Looney discovered that						A-PUL PULS- 03071	
Uncontroll ed Resource Consumpti on	18-0	6-2019	5	the TCI implem in the I fragme certain Acknow sequen could uservice stable I 4.9.182 and is ff f070ef2 baf55f8	Pretransinentation in the control who the cont	emission in tcp_rnel coulon hand ective ent (SAC emote at o cause as been feleases 427, 4.19. commit 635706	i queue fragmer ld be lling K) tacker a denial ixed in 4.4.182, 52, 5.1.1	of 11,	ww ogy sec adv Syr SA_	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-PUL PULS- 03071	
Uncontroll ed Resource Consumpti	18-0	6-2019	5	the Lin	an Loone ux kerne oded to a remote	el defaul 48 bytes	t MSS is . This		ww	ps://w v.synol v.com/ urity/	A-PUL PULS- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID
on				more the enforce use this service stable leads of the service of t	send quenan if a led. A rement of the caus	arger M note atta e a deni s been f eleases 4 27, 4.19. commits e6e5d7d and 214781	SS were acker con al of ixed in4.182, 5.1.1805e19	uld 11, 95b	Syn	risory/ nology_ 19_28		
pulse_policy	z_secu	ire										
Integer Overflow or Wraparou nd	18-0	6-2019	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 88ed1a2f78cff.  CVE ID: CVE-2019-11477					ogy sec adv Syn	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-PUL PULS- 03071	- 9/354
Uncontroll ed Resource Consumpti on	18-0	6-2019	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,					ogy sec adv Syn	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-PUL PULS- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-	.7	7-8	8-9	9-10

Weakness	Publis	h Date	cvss		Descript	ion & CV	E ID		F	Patch	NCIIF	PC ID
				and is f f070ef2 baf55f8	2, 4.14.12 fixed in c 2ac6671 3191a2e	ommit 635706	6b683fb	·				
Uncontroll ed Resource Consumpti on	18-06-	-2019	5	Jonatha the Lin hard-co allows TCP res more the enforce use this service stable la 4.9.182 and is f 967c05 3a20ef 5f3e2b b4654h	an Loone ux kerne oded to 4 a remote send que han if a led. A rem s to caus to	ey discovel default 48 bytes e peer to eues signarger Manote attace a deni s been feleases 427, 4.19. commits e6e5d76 and 214781	vered the t MSS is a This of fragmen ificantly SS were also of E.4.182, 52, 5.1.1	ent y uld	ogy sec adv Syr	ps://w z.synol z.com/ urity/ zisory/ nology_ 19_28	A-PUL-PULS-03071	
pulse_conn	ect_seci	ure										
Integer Overflow or Wraparou nd	18-06-		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 88ed1a2f78cff.  CVE ID: CVE-2019-11477					ww ogy sec adv Syr SA_	ps://w v.synol v.com/ urity/ visory/ nology_ 19_28	A-PUL-PULS-03071	9/357
Uncontroll  CV Scoring S				Jonathan Looney discovered that				at	htt	ps://w	A-PUL-	
(CVSS)	caie	0-1	1-2	2-3 3-4 4-5 5-6					-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
ed Resource Consumpti on			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 f070ef2ac66716357066b683fb0 baf55f8191a2e.  CVE ID: CVE-2019-11478	ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	PULS- 030719/358
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-PUL- PULS- 030719/359
n li			CVE ID : CVE-2019-11479		
Pydio cells					
CCIIS			Pydio Cells before 1.5.0 fails to		
N/A	19-06-2019	6.5	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
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		Pa	tch	NCII	PC ID
			_	ileged di ge escala	-	leading	to				
			CVE ID	: CVE-2	019-12	901					
Informatio n Exposure	19-06-2019	4	incomp data up new us ID as a the del		nup of a tion. Thi ng the s user, to r's data.	a user's s allows ame Use restore		N/A		A-PYD CELL- 03071	
Informatio n 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- 03071	
Qemu											
qemu											
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command	24-06-2019	10	QEMU vulnera injection remote execution inform sending to the l	e QMP migrate command in MU version 4.0.0 and earlier is nerable to OS command ection, which allows the note attacker to achieve code cution, denial of service, or ormation disclosure by ding a crafted QMP command he listening server.				N/A		A-QEN QEMU 03071	-
Improper Neutralizat ion of Special Elements used in an OS	24-06-2019	10	QEMU to OS c allows code ex or info	IP guest 4.0.0 and ommand the attack ecution rmation g a crafte	d earlier l injection cker to a , denial o disclosu	e,	N/A		A-QEMU QEMU 03071	-	

(CVSS)

Weakness	Publish Date	cvss		Descripti	on & CV	E ID		F	atch	NCII	PC ID						
Command ('OS Command Injection')			to the li			929											
quadbase																	
espressrep	ort_es																
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-06-2019	3.5	to executand injection into the payload new usernar stored payload triggers. Security User/Gill the at have performed the payload payl	Report 7 allows ate mali- ect arbit etarget p l is store er accou me to an payload ed by acc y Levels roup Re etacker co ermissio	ES (ERE s remote cious Jav rary sou pages. The d by cre nt, and s XSS pay can the cessing to lationsh loes not n to cre ulnerabi	(S) v7.0 e attacked vaScript urce code he XSS eating a setting to yload. The betthe "Set	ee hee ne ne lly w	N/A	A	A-QUA ESPR- 03071	A- 9/365						
Radare			CVE ID	: CVE-2	019-99	57											
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	A-RAD RADA 03071							
rdkcentral																	
rdkb_ccspp	andm																
Improper Neutralizat ion 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					cosa_wifi_apis.c in the RDK RDKB-20181217-1 CcspWifiAgent module allows			cosa_wifi_apis.c in the RDK RDKB-20181217-1 CcspWifiAgent module allows		S	N/A	A	A-RDI- RDKB- 03071	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10						

Weakness	Publish Date	cvss	Description & CVE ID	P	Patch	NCIIPC ID
used in a Command ('Comman d 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		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 disclosur and code execution by crafting a 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 WebUfmodules.	re n N/A	A	A-RDK- RDKB- 030719/369
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publ	ish Date	cvss		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
				CVE ID : CVE-2019-6964								
Redhat												
cloudforms	_mana	agement	_engin	е								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-0	6-2019	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					ugz dha /sh g.cg VE-	ps://b zilla.re at.com low_bu gi?id=C -2019- 177	A-RED CLOU- 03071	
enterprise_	linux_	atomic_	host									
Integer Overflow or Wraparou nd	18-00	6-2019	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 88ed1a2f78cff.				ogy sec adv Syr	ps://w z.synol z.com/ urity/ visory/ nology_ 19_28	A-RED ENTE- 03071		
Uncontroll ed Resource Consumpti on		6-2019	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					ogy sec adv	ps://w v.synol v.com/ urity/ visory/ nology_	A-RED ENTE- 03071	
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-	6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
			sequent could we service stable le 4.9.182 and is for 10 f	wledgme ces. A re se this to This ha kernel re 2, 4.14.12 fixed in c 2ac6671 3191a2e	emote at o cause as been f eleases 4 27, 4.19. commit 635706	tacker a denial ixed in .4.182, 52, 5.1.1	l1,	SA	19_28		
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.						ps://w v.synol v.com/ ourity/ visory/ nology_ _19_28	A-RED ENTE- 03071	
enterprise_	mrg										
Integer Overflow or Wraparou nd	18-06-2019	7.8	the TCl >tcp_gs to an ir Linux l Selectiv (SACKs use this service stable l 4.9.182	an Loone P_SKB_C so_segs wateger over kernel water so A rem so to caus a. This ha kernel re 2, 4.14.12	B(skb)- value wa verflow i hen han owledgm ote attac e a deni as been f eleases 4 27, 4.19.	et CP ild	ogy sec adv Syr	ps://w v.synol v.com/ urity/ visory/ nology_ _19_28	A-RED ENTE- 03071		
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			3b4929f65b0d8249f19a50245cd 88ed1a2f78cff.		
			CVE ID : CVE-2019-11477		
Uncontroll ed Resource Consumpti on	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 f070ef2ac66716357066b683fb0 baf55f8191a2e.	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-RED- ENTE- 030719/375
			CVE ID : CVE-2019-11478		
Uncontroll ed Resource Consumpti on	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 3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5c b4654b9fc363.	https://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_28	A-RED- ENTE- 030719/376
1 11			CVE ID : CVE-2019-11479		
redwoodhq					
redwoodhq					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1	12	2 3	3 4	7 3	3 0	0 /	, 0	0 3	3 10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	PC ID		
Improper Authentica tion	19-0	6-2019	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	A-RED REDW 03071	-		
Rubygems														
rubygems														
Argument Injection or Modificatio n	17-0	6-2019	5	RubyGo 3.0.2. S Gem::U calls sa sequen	e was diems 2.6 aince serInter y withouce inject : CVE-2	and later action# it escaption is po	r throug verbose ing, esca		N/A	A	A-RUB RUBY- 03071			
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection' )	17-0	6-2019	5	RubyGo 3.0.2. T outputs respon Therefo crafted injection	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	A-RUB RUBY- 03071				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m	17-0	6-2019	5	An issue was discovered in RubyGems 2.6 and later through 3.0.2.  Gem::GemcutterUtilities#with_re sponse may output the API response to stdout as it is.  Therefore, if the API side modifies the response, escape sequence injection may occur.			RubyGems 2.6 and later through 3.0.2. Gem::GemcutterUtilities#with_re sponse may output the API response to stdout as it is. Therefore, if the API side modifies the response, escape		Gems 2.6 and later through: GemcutterUtilities#with_re se may output the API onse to stdout as it is. efore, if the API side fies the response, escape		N/A	A	A-RUB RUBY- 03071	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6	5-7	7-8	8-9	9-10		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Componen t ('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 multiline 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 Dereferenc e	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://w ww.synol ogy.com/ security/ advisory/ Synology_ SA_19_27	A-SAM- SAMB- 030719/383
NULL Pointer Dereferenc e	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://w ww.synol ogy.com/ security/	A-SAM- SAMB- 030719/384
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	7-8	8-9 9-10

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		F	Patch	NCIII	C ID
			to an attacker using the paged search control. The attacker must have directory read access in order to attempt an exploit.				Syn	risory/ rology_ 19_27			
			CVE ID	: CVE-2	019-12	436					
Seeddms											
seeddms											
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	20-06-2019	6	Remote (RCE) t upload vulnera 12940.	MS before Command Control of PHP stability the second control of t	and Exec of unval scripts, a an CVE-	cution idated fi differen		our e.no eed ode aste	ps://s rceforg et/p/s dms/c e/ci/m er/tree HANGE	A-SEE- 03071	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-06-2019	3.5	before Cross-S name fi	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				our e.no eed ode	ps://s rceforg et/p/s dms/c e/ci/m er/tree HANGE	A-SEE- 03071	
Improper Neutralizat ion 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	A-SEE- 03071		
Shopware											
shopware											
Improper	23-06-2019	4.3	Shopware before 5.5.8 has XSS					N/A		A-SHO-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Weakness	Publ	ish Date	CVSS		Descript	ion & CV	E ID		ı	Patch	NCIII	PC ID
Neutralizat ion of Input During				via the Query String to the backend/Login or backend/Login/load/ URI.  CVE ID: CVE-2019-12935							SHOP- 03071	9/388
Web Page Generation ('Cross-site Scripting')				CVEID	: CVE-2	019-12	933					
Symantec												
data_loss_p	reven	tion										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-0	6-2019	3.5	version cross-s vulnera can ena client-s viewed site scr be used access origin p	is MP1 as may be ite scrip ability, a ability, a ability, a be scrip by othe ipting vertical by attacontrols colicy.	e suscepting (XS type of ckers to ots into r users. alnerabickers to such as	otible to S) issue the inject web pag A cross- lity may bypass the sam	at ges -	N/A	A	A-SYM DATA- 03071	
Tenable												
nessus												
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	25-0	6-2019	4.3	Nessus versions 8.4.0 and earlier were found to contain a reflected XSS vulnerability due to improper validation of usersupplied 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			ed ker	le.c	ps://w v.tenab com/se rity/tns 119-04	A-TEN NESS- 03071		
twistedmatrix												
twisted												
CV Scoring S (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-06-2019	In words.protocols.jabber.xmlstrea m 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
ultimateme	ember				
ultimate_m	ember				
Weak Password Recovery Mechanis m 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

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1	12	2 3	7	7	5	0 7	7-0	5	3 10

Weakness	Publish Date	CVSS		Descripti	on & CVI	E ID		F	Patch	NCIIF	PC ID
			picture perform first ne interce request parame	the profess of priven such a eds to (for an up and mother.	ileged u modific or exam load-pic dify the	sers. To ation, on ple) cture user_id	ne				
Videolan											
vlc_media_p	olayer										
Double Free	18-06-2019	7.5	zlib_dec module VideoL through demuxe malforn double	e was di compres s/demu AN VLC n 3.0.7. T er, while med MK free. : CVE-2	s_extra x/mkv/ media p 'he Mati parsing / file typ	in util.cpp layer 3.x oska g a oe, has a	X	N/A	A	A-VID- 03071	
Zohocorp											
manageeng	ine_servicede	sk_plus	3								
N/A	18-06-2019	7.2	product privileg improp %SYST e direct Moreov with sa binarie current start. The privileg	e Zoho Mets suffer ge escalar er permeter and cory and co	from lo tion due issions factorizes ervices access try to see section of the factorize to t	cal e to for the nageEng folders. associat co execu from the system ly allow escalate	ced te	www gee con uct top cen eva of- pri	ps://w v.mana engine. n/prod s/desk destral/el etral/el etral/el etral/el	A-ZOH MANA- 03071	-
			affects EventL Service	RITY\S! Desktop og Analy Desk Plu tCenter	zer 12.0 is 10.0.0	10.0.38 ).2, ),	30,		html		

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		
manageeng	ine_analytics_ <sub>]</sub>	plus			
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0,	https://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.html	A-ZOH- MANA- 030719/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
manageeng	ine_browser_s	ecurity	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		
manageeng		Cearre			
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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 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://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.html	A-ZOH- MANA- 030719/397
	ine_desktop_c				
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine	https://w	A-ZOH-
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Descript	ion & CVI	E ID		P	atch	NCII	PC ID
			privilegimprop %SYST e direct Moreov with sa binarie current start. T non-pr privileg AUTHO affects EventL Service Suppor Manage Manage Connec Manage Manage T2.3, N OpUtils Configu FireWa 5.6, Pas Analyti Securit	ts suffer ge escalar er perm EMDRIV tory and ver, the sid produst such as the directory of the suffer of the suffer Plus 9 of the Plus 9 of th	from loadissions of the control of t	cal cal cat	ed te e e e e e e e e e e e e e e e e e	www gee com ucts top cen eva of- priv vuli	.mana ngine. n/prod s/desk	MANA	
manageeng	ine_eventlog_a	ınalyze	er								
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the			ed te	www gee com ucts top cen	os://w .mana ngine. n/prod s/desk - tral/el tion-	A-ZOF MANA 03071		
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4 140	4-5	5-6	6-	-7	7-8	8-9	9-10

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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability 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- vulnerabil ity.html	
manageeng	ine_firewall				
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.html	A-ZOH- MANA- 030719/400

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SupportCenter Plus 8.1, 0365 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		
manageeng	ine_key_mana	ger_plı			
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network	https://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.html	A-ZOH- MANA- 030719/401

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  Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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, 0365 Manager Plus 9.0.0, Patch Manager Plus 9.0.0, Patch Manager Plus 9.0.0, Opthanager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager Plus 5.6, Password Manager Plus 5.6, Passwo	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%/ManageEngin e 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, 0365 Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Connect Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager Plus 9.0.0, PireWall 12.0, Key Manager Plus 5.6, Password Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus.  CVE ID: CVE-2019-12133	manageeng	ine_mobile_de	vice_m	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  anager_plus		
manageengine_network_configuration_manager				products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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, 0365 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.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil	MANA-

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

Weakness	Publish Date	cvss		Descripti	ion & CV	E ID		F	Patch	NCII	PC ID
N/A	18-06-2019	7.2	produce privileg impropers of the control of the co	le Zoho Mets suffer ge escala per perm l'EMDRIV tory and ver, the said products such as t directo l'his will es such as t directo l'his will es to NTORITY\SY Desktop log Analy et Plus 4 er Plus 4 er Plus 9 et Plus 9 et Plus 9 et Plus 9 et Flow A said 12.0, Nouration Mets sword Mets l'es Plus 12.0, Nouration Mets l'es Plus 12.0, Hessword Mets l'es Plus 12.0, Hessword Mets Plus 12.0, Hessword Mets Plus 12.0, Hessword Mets Plus 12.0, Hessword Mets l'es Plus 12.0, Hessword Mets 12.0, Hessword Me	from lo tion due issions a E%\Ma its subservices acts try to secretary upon effective users to EYSTEM. Central exer 12.0 Plus 8.1 .0, Mobil. 0.0, Pat .0.0, Oplat. 0.0, Oplat. 0.0, Oplat. 0.0, Oplat. 0.0, Oplat. 0.0, and Exervices and Exercises and Exerci	cal e to for the mageEng folders. associate to execu from the system ely allow escalate This 10.0.38 0.2, 0, 0, 0365 le Device ch merabilite ch Manager 11.0, 11.0, ager Plue Pro 9.9 Browser	ted te e e e e e e e e e e e e e e e e e	www gee con uct top cen eva of- priv vul	ps://w v.mana engine. n/prod s/desk - tral/el tion- vilege- nerabil html	A-ZOH MANA 03071	
manageeng	ine_o365_man	ager_p	lus								
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e directory and its sub-folders.  Moreover, the services associated with said products try to execute			ted	www gee con uct top cen	ps://w v.mana engine. n/prod s/desk - tral/el tion-	A-ZOH MANA 03071		
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-	.7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability 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.	of- privilege- vulnerabil ity.html	
manageeng	ine_opmanage	r			
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.html	A-ZOH- MANA- 030719/405

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, 0365 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		
manageeng	ine onutils		CVE ID . CVE-2019-12133		
manageeng	mc_oputiis		Multiple Zoho ManageEngine		
N/A	18-06-2019	7.2	products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0,	https://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.html	A-ZOH- MANA- 030719/406

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

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
manageeng	ine_password	manas	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		
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus.  CVE ID: CVE-2019-12133	https://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.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%\ManageEngin e 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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Patch Connect Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus.  CVE ID: CVE-2019-12133	https://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.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%\ManageEngin e directory and its sub-folders. Moreover, the services associated	https://w ww.mana geengine. com/prod ucts/desk top- central/el	A-ZOH- MANA- 030719/409			
CV Scoring S (CVSS)	cale 0-1	1-2	<b>2-3 3-4 4-5 5-6 6</b>	5-7 7-8	8-9 9-10			

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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus.	evation- of- privilege- vulnerabil ity.html	
manageeng	ine_supportce	nter_p	lus		
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.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, 0365 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.		
manageeng	ine_vulnerabil	ity ma	CVE ID : CVE-2019-12133		
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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, 0365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, OpManager	https://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.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		
manageeng	ine_adselfserv	ice_plu	IS		
Improper Authentica tion	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
manageeng	ine_netflow_a	nalyzei			
N/A	18-06-2019	7.2	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngin e 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://w ww.mana geengine. com/prod ucts/desk top- central/el evation- of- privilege- vulnerabil ity.html	A-ZOH- MANA- 030719/413

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SupportCenter Plus 8.1, 0365 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