

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

01 - 15 Oct 2019

Vol. 06 No. 19

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Application		
activesoft					
mybuilder					
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	07-10-2019	7.5	ActiveX Control in MyBuilder before 6.2.2019.814 allow an attacker to execute arbitrary command via the ShellOpen method. This can be leveraged for code execution CVE ID: CVE-2019-12811	N/A	A-ACT- MYBU- 221019/1
Improper Input Validation	07-10-2019	7.5	MyBuilder viewer before 6.2.2019.814 allow an attacker to execute arbitrary command via specifically crafted configuration file. This can be leveraged for code execution. CVE ID: CVE-2019-12812	N/A	A-ACT- MYBU- 221019/2
adhouma_cm	s_project				
adhouma_cm	s				
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	10-10-2019	7.5	Adhouma CMS through 2019- 10-09 has SQL Injection via the post.php p_id parameter. CVE ID: CVE-2019-17429	N/A	A-ADH- ADHO- 221019/3
Apache					
mina					
Cleartext	01-10-2019	5	Handling of the close_notify	N/A	A-APA-
CV Scoring Scal (CVSS)	e 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
Transmissio n of Sensitive Information			SSL/TLS message does not lead to a connection closure, leading the server to retain the socket opened and to have the client potentially receive clear text messages afterward. Mitigation: 2.0.20 users should migrate to 2.0.21, 2.1.0 users should migrate to 2.1.1. This issue affects: Apache MINA. CVE ID: CVE-2019-0231		MINA- 221019/4
awplife					
contact_form	_widget				
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	10-10-2019	7.5	The new-contact-form-widget (aka Contact Form Widget - Contact Query, Form Maker) plugin 1.0.9 for WordPress has SQL Injection via all-query-page.php. CVE ID: CVE-2019-17072	N/A	A-AWP- CONT- 221019/5
axiosys					
bento4					
NULL Pointer Dereference	10-10-2019	4.3	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListInspector:: Action in Core/Ap4Descriptor.h, related to AP4_IodsAtom::InspectFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4dump. CVE ID: CVE-2019-17452	N/A	A-AXI-BENT- 221019/6
NULL Pointer Dereference	10-10-2019	4.3	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListWriter::Act ion in Core/Ap4Descriptor.h,	N/A	A-AXI-BENT- 221019/7
CV Scoring Scal (CVSS)	le 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				
			related to AP4_IodsAtom::WriteFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4encrypt or mp4compact. CVE ID: CVE-2019-17453						
NULL Pointer Dereference	10-10-2019	4.3	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_Descriptor::GetTag in Core/Ap4Descriptor.h, related to AP4_StsdAtom::GetSampleDes cription in Core/Ap4StsdAtom.cpp, as demonstrated by mp4info. CVE ID: CVE-2019-17454	N/A	A-AXI-BENT- 221019/8				
bludit									
bludit									
Improper Restriction of Excessive Authenticati on Attempts	06-10-2019	4.3	bl-kernel/security.class.php in Bludit 3.9.2 allows attackers to bypass a brute-force protection mechanism by using many different forged X-Forwarded-For or Client-IP HTTP headers.	N/A	A-BLU- BLUD- 221019/9				
			CVE ID : CVE-2019-17240						
bootstrap-3-t	ypeahead_pro	oject							
bootstrap-3-t	ypeahead								
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	08-10-2019	4.3	Bootstrap-3-Typeahead after version 4.0.2 is vulnerable to a cross-site scripting flaw in the highlighter() function. An attacker could exploit this via user interaction to execute code in the user's browser. CVE ID: CVE-2019-10215	https://bu gzilla.redh at.com/sho w_bug.cgi?i d=CVE- 2019- 10215	A-B00- B00T- 221019/10				
butor									
CV Scoring Scal (CVSS)	le 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	NCIIPC ID	
portal										
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-10-2019	5	Butor Portal before 1.0.27 is affected by a Path Traversal vulnerability leading to a preauthentication arbitrary file download. Effectively, a remote anonymous user can download any file on servers running Butor Portal. WhiteLabelingServlet is responsible for this vulnerability. It does not properly sanitize user input on the theme t parameter before reusing it in a path. This path is then used without validation to fetch a file and return its raw content to the user via the /wl?t=//&h= substring followed by a filename. CVE ID: CVE-2019-13343				buc. /bu tear al/c s/al http buc. /bu tear al/s 055 4fcf ee1 a9cc java butc al/v vlet Lab rvle	n/port commit l, os://bit ket.org	A-BUT PORT- 22101	
CA										
network_flow	_analysis									
Use of Hard- coded Credentials	02-10-2019	7.5	CA Network Flow Analysis 9.x and 10.0.x have a default credential vulnerability that can allow a remote attacker to execute arbitrary commands and compromise system security. CVE ID: CVE-2019-13658						A-CA-N 22101	
Centreon	L									
centreon_vm										
Reliance on Cookies without	08-10-2019	5	In Centreon VM through 19.04.3, the cookie configuration within the			N/A	N/A		-	
CV Scoring Sca (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	NCII	PC ID
Validation and Integrity Checking			Apache HTTP Server does not protect against theft because the HTTPOnly flag is not set. CVE ID: CVE-2019-17104						22101	9/13
centreon_web)								L	
Cleartext Storage of Sensitive Information	08-10-2019	4	2.8.29 compo allows to mo compo	In Centreon Web through 2.8.29, disclosure of external components' passwords allows authenticated attackers to move laterally to external components. CVE ID: CVE-2019-17106				1	A-CEN CENT- 22101	
Checkpoint										
security_gate	way									
Improper Handling of Exceptional Conditions	02-10-2019	5	R80.3 before by Che Manag uniqu enhan	In a rare scenario, Check Point R80.30 Security Gateway before JHF Take 50 managed by Check Point R80.30 Management crashes with a unique configuration of enhanced logging. CVE ID: CVE-2019-8462				1	A-CHE SECU- 22101	
Cisco										
adaptive_secu	ırity_appliano	e_soft	ware							
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker				n N/A		A-CIS- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCII	PC ID
			by sentraffice. The avalid auther address stater applies of the exploattack memory arelows.	exploit and an aftacker of credenticate to exploit and the exploit and the exploit could according to exploit could according to exploit and of an an according to the exploit could according to exploit and of an according to exploit and according to exploit according to exploit and according to exploit and according to exploit according to exploit and according to exploit according to explority according to exploit a	ee ee					
unified_comm	nunications_i	nanage	er							
Inconsistent Interpretatio n of HTTP Requests ('HTTP Request Smuggling')	02-10-2019	6.4	A vulnerability in the webbased interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to bypass security restrictions. The vulnerability is due to improper handling of malformed HTTP methods. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. A successful exploit could allow the attacker to gain unauthorized access to the system. CVE ID: CVE-2019-15272				f N/	A	A-CIS- 22101	
Improper Neutralizatio n of Input	02-10-2019	4.3	A vulnerability in the web- based interface of multiple Cisco Unified Communications					A	A-CIS-UNIF- 221019/18	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					Patch	NCIII	PC ID
During Web Page Generation ('Cross-site Scripting')			unaut attack site so agains based softw due to user-s web-k affect could by per interf A succ allow arbitr conteri interf brows	icts coulchenticated to concern the concer	ted, remoduct a (XSS) attacked of the waller action to a terface of the terface o	ote cross- tack veb- affected bility is idation of y the of the attacker nerability of the fited link ould execute n the l nsitive nation.	of - y			
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-10-2019	4	based Unified Manay Comm Session (SME) authe to implead an affer execut queric exists softw user-s queric exploisending	A vulnerability in the webbased interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an authenticated, remote attacker to impact the confidentiality of an affected system by executing arbitrary SQL queries. The vulnerability exists because the affected software improperly validates user-supplied input in SQL queries. An attacker could exploit this vulnerability by sending crafted requests that contain malicious SQL				A	A-CIS-1 22101	
CV Scoring Scal (CVSS)	e 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
			application. A successful exploit could allow the attacker to determine the presence of certain values in the database, impacting the confidentiality of the system. CVE ID: CVE-2019-12710		
Improper Restriction of XML External Entity Reference ('XXE')	02-10-2019	6.4	A vulnerability in the webbased interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to access sensitive information or cause a denial of service (DoS) condition. The vulnerability is due to improper restrictions on XML entities. An attacker could exploit this vulnerability by sending malicious requests to an affected system that contain references in XML entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a DoS condition. CVE ID: CVE-2019-12711	N/A	A-CIS-UNIF- 221019/20
Improper Neutralizatio n of Input During Web Page Generation	02-10-2019	4.3	A vulnerability in the web- based interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition	N/A	A-CIS-UNIF- 221019/21
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID					Patch	NCIII	PC ID
('Cross-site Scripting')			unaut attack site so agains based softw due to user-s web-k affect could by perinterf A succallow arbitr content interf brows	could a chenticat cer to concripting of st a user interfact are. The consuffice supplied coased interest ed softwe exploit of resuading face to clip cessful entranged the attack cary scrip ext of the face or accept as ser-base D: CVE-	ted, remoduct a (XSS) at of the water of the vulneraction to the control of the c	cross- tack veb- affected bility is idation of the attacker aerability of the fted link ould execute n the l nsitive nation.	of y			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	based Unified Manay Comm Session (SME) unaut attack site so agains based vulne insuff suppl based softw explore	A vulnerability in the webbased interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to conduct a cross- site scripting (XSS) attack against a user of the web- based interface. The vulnerability is due to insufficient validation of user- supplied input by the web- based interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the				A	A-CIS-1 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	e CVSS		Description & CVE ID				atch	NCIIF	PC ID
			allow arbiticonte interf brow	the attactary scriptext of the face or actact ser-base	cker to e ot code i affected ccess ser d inforn 2019-1					
Cross-Site Request Forgery (CSRF)	02-10-201	4.3	Unifice Mana Command Fine Comma	based interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition (SME), Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross- site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections by the affected software. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could change the password of a targeted user. An attacker could then take unauthorized actions on behalf of the targeted user.					A-CIS-1 22101	
firepower_ma	nagement_	center								
Improper Neutralizatio	02-10-201	9 9		Multiple vulnerabilities in the web-based management					A-CIS-I	FIRE-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4			6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss			Patc	h	NCIII	PC ID			
n of Special Elements used in an SQL Command ('SQL Injection')			Manage Softwall auther to execute that in of the	ace of Cigement of are could nticated ecute arbitions on a ce. These due to in atton. And it these was crafted de it could a cer to vie hey are make changed to the commolying openay affect device. D: CVE-	Center (d allow a , remote itrary Se an affect vulnera attacke vulneral ed SQL q vice. A s allow the ew inform anges to anges to ands wi erating t the ava-	FMC) an e attacked QL ed bilities input r could bilities b ueries t uccessfie mation orized t o the hot ithin the system ailability	y o ul o			22101	9/24
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-10-2019	9	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the				er N/ y o ul	'A		A-CIS-1 22101	
CV Scoring Scal (CVSS)	e 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
			system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device. CVE ID: CVE-2019-12680 Multiple vulnerabilities in the web-based management		
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-10-2019	9	interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device. CVE ID: CVE-2019-12681	N/A	A-CIS-FIRE- 221019/26
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL	02-10-2019	9	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected	N/A	A-CIS-FIRE- 221019/27
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
Injection')			device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device. CVE ID: CVE-2019-12682		
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-10-2019	9	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability	N/A	A-CIS-FIRE- 221019/28

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			of the device. CVE ID : CVE-2019-12683		
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-10-2019	9	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to an affected device. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, and execute commands within the underlying operating system that may affect the availability of the device. CVE ID: CVE-2019-12684	N/A	A-CIS-FIRE- 221019/29
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-10-2019	9	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary SQL injections on an affected device. These vulnerabilities exist due to improper input validation. An attacker could exploit these vulnerabilities by sending crafted SQL queries to	N/A	A-CIS-FIRE- 221019/30
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pul	blish Date	CVSS		Descript	ion & CV	E ID		Patch	NCIII	PC ID
				explo attack that the view, system author execurunder that nof the	ected de it could a cer to vie hey are i make che it rized to te comme clying operay affect device. D: CVE-	allow thew informot authors anges to make, ands we rating at the averating	e mation orized to the not ind ithin the system ailability	0			
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-	10-2019	9	Multiple web-less interformana, Software authors and affect of the service of the	ple vulno pased ma ace of Ci gement are coul nticated cute arb ions on a e. These due to in it these varied acted de it could a ected de it could a hey are in make ch make ch make ch make ch mithat the rized to te commander of device. D: CVE-	erabilition anagement of sco Fire Center (dallow premote an affect vulneration of such as allow the ewinform of authors and swaperating with the available with the a	es in the ent power FMC) an eattacked bilities input or could bilities be ueries to the not ent in the system ailability	er o N/A o	A	A-CIS- 22101	
Improper Restriction of	02-	10-2019	9	the Ci	A vulnerability in the web UI of the Cisco Firepower Management Center (FMC)				Α	A-CIS- 22101	
CV Scoring Scal (CVSS)	e	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
Operations within the Bounds of a Memory Buffer			could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary commands within the affected device. CVE ID: CVE-2019-12687		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-10-2019	9	A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary commands within the affected device. CVE ID: CVE-2019-12688	N/A	A-CIS-FIRE- 221019/33
Improper Input Validation	02-10-2019	9	A vulnerability in the web- based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system of an affected device.	N/A	A-CIS-FIRE- 221019/34
CV Scoring Scal (CVSS)	e 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
			The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending malicious commands to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device. CVE ID: CVE-2019-12689		
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	02-10-2019	9	A vulnerability in the web UI of the Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to inject arbitrary commands that are executed with the privileges of the root user of the underlying operating system. The vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input in the web UI. A successful exploit could allow an attacker to execute arbitrary commands on the device with full root privileges. CVE ID: CVE-2019-12690	N/A	A-CIS-FIRE- 221019/35
Improper Limitation of a Pathname to a Restricted Directory ('Path	02-10-2019	4	A vulnerability in the web- based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to perform a directory	N/A	A-CIS-FIRE- 221019/36
CV Scoring Scale (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

	ish Date CVS	S	Description	on & CVE	ID	Pa	itch	NCIIF	PC ID
Traversal')		device to instance by the mana attack vulne crafte web-linters could by passecuracces	ersal attactions. The vulue sufficient e web-based gement in the could be a sed mandate of the could be a sed mandate. A such allow the sed the could be a sed mandate of the could be a s	Inerabili input va sed nterface exploit by sendir request t anageme ccessful e attacke MC Softwortions ar					
Uncontrolled Resource Consumption	0-2019 6.8	A vulconfig Authoused Threa Softw Mana Softw authoused (DoS) vulnoused impromana user s attack vulnoused an aff perfo simul Secur	nerability guration of entication in Cisco Fat Defense vare, Cisco egement (vare, and vare could enticated, use a denicated, use a denicated erability is oper resongement in session maker could erability befected systematical erability before a shell (Section 2016).	y in the of the Plan Module Firepower (FTD) or Firepower (FC) or Firepower (FC) or Firepower (FC) or The or The contanagem exploit for the contanagem exploi	uggable e (PAM) er wer eMC) OS n attacker vice htext of ent. An this cting to ul ns. A	N/A		A-CIS-I 22101	
			essful exp ttacker to						

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		Patch	NCIII	PC ID
			to relected to rel	D : CVE - nerabilit are insp	alting in exploit to the atta ser credo 2019-1 y in the ection for	on f				
Improper Input Validation	02-10-2019	5	allow remote file are polici. The vecau insuff income could by sere reque device could bypas inspecemalic.	Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass the file and malware inspection policies on an affected system. The vulnerability exists because the affected software insufficiently validates incoming traffic. An attacker could exploit this vulnerability by sending a crafted HTTP request through an affected device. A successful exploit could allow the attacker to bypass the file and malware inspection policies and send malicious traffic through the affected device.				'A	A-CIS- 22101	
prime_infrast	ructure									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	based of Ciscould unaut attack site so again: based	nerabilit manage co Prime allow ar chenticat ter to co cripting st a user manage affected	ement in e Infrast n ed, rem nduct a (XSS) at of the w	terface ructure ote cross- tack veb- terface	N/	'A	A-CIS- 22101	
CV Scoring Scal (CVSS)	e 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
			vulnerability is due to insufficient validation of user-supplied input in multiple sections of the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	A vulnerability in the webbased management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to conduct a crosssite scripting (XSS) attack against a user of the webbased management interface of the affected software. The vulnerability is due to insufficient validation of usersupplied input by the webbased management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based	N/A	A-CIS-PRIM- 221019/40

Weakness	Publish Date	cvss		Descript	F	atch	NCIII	PC ID		
			inforr	nation.						
			CVE I	D : CVE-	2019-1	2713				
unified_comm	nunications_n	nanage	r_im_a	nd_pres	ence_se	ervice				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	based Cisco produ unaut attack site so agains based softw due to user-s web-k affect could by per interf A succ allow arbitr conterinterf brows	interface Unified (Interface Unified (Interface Interf	ce of much deallow and allow and allow and allow and allow and allow are of the will are face of the are. An and allow are are and allow are are are and allow are	Itiple nication an ote cross- tack reb- affected bility is idation of y the of the attacker herability of the fted link ould execute n the l nsitive nation. 2707	of N/A		A-CIS-1 22101	
Cross-Site Request Forgery (CSRF)	02-10-2019	4.3	A vulnerability in the web-based interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition (SME), Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-						A-CIS-1 22101	
CV Scoring Scal	e 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
			site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections by the affected software. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could change the password of a targeted user. An attacker could then take unauthorized actions on behalf of the targeted user. CVE ID: CVE-2019-1915		
adaptive_secu	ırity_applianc	e			
Improper Input Validation	02-10-2019	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device. CVE ID: CVE-2019-12673	N/A	A-CIS-ADAP- 221019/43

Weakness	Publish Date	cvss		Descripti	on & CVI	EID	F	atch	NCII	PC ID
Improper Input Validation	02-10-2019	3.3	Shorte imple Adapt (ASA) Firepo (FTD) unaut attack affecte denial condirexists software attack affected at a state a 11 pare explores endirected could cause device condirected is trav	chenticated deviced deviced deviced lof serviced because are impropered advertised logonal devertised a reloaded resultion for eversing to the control of th	First (Oon of Cistrity Appres and Circat Define a could lead, adjactions and compared to the affect of the and affect of the and affect of the and a could lie attack of the and a could l	SPF) co coliance isco ense allow and cent oad of and ing in a ceted carses PF link- LSA) type er could ity by type 11 ected caploit er to affected cos affic that ee.	n N/A		A-CIS- 22101	
Improper Handling of Exceptional Conditions	02-10-2019	4	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-						A-CIS- 22101	
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		Descript	ion & CVI	EID	Pa	atch	NCII	PC ID
			could by op session the afthis view of the afthis connection of the succession o	ening mand tracker walid used fected designated and ser to over allocated to ondition of the condition of th	this vulnary SSL affected would not be received to allow the erwrite ry location errought to features. Establications L/TLS affected vulnerary locations affected would affect wou	derability VPN I device. Heed to Hitals on Hit				
Integer Underflow (Wrap or Wraparound	02-10-2019	5	Initiations in special (ASA) Firepo (FTD) unaut	nerability tion Protection modelive Secu Softwar Softwar Softwar Chenticat Sec (DoS)	tocol (SI dule of drity Appre and Ci reat Def re could ted, remouse a dec	N/A		A-CIS- 22101		
CV Scoring Scal	e 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		Pa	tch	NCIII	PC ID
			vulne impro messa explo sendi throu succe the at intege softw unma result	ed device rability in per parsenges. An it this worden an affect of the control o	is due to sing of S attacker alnerabil icious S fected de bloit cou b trigger flow, car y to reac emory a crash.	IP could lity by IP packe evice. A ld allow an using the	,				
Incorrect Type Conversion or Cast	02-10-2019	4	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash. CVE ID: CVE-2019-12693				y N	/A		A-CIS- 22101	
Improper Neutralizatio	02-10-2019	4.3	A vulnerability in the Clientless SSL VPN (WebVPN)			N	/A		A-CIS- 22101		
CV Scoring Scal (CVSS)	e 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		Descripti	ion & CV	E ID	Р	atch	NCIII	PC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Secur Cisco Defen allow remote cross- attack web-k interf The v insuff suppl based of an a attack vulne user of crafte exploi attack script the in attack script the in attack	an unaute attack site script against ased made of an ulnerabicient valid input affected arability before the interface of accept to accept acc	ance (A rer Thre) Softwa thentica er to con pting (X a user of anagement affected lity is do lidation t by the ement in device. A l exploit by persu erface to success allow the ecute ar the cont or allow cess sen d inform	SA) and at at are could ated, and at a SS) of the ent at a device. The area at a could ated at a state at a could ate a state at a could atea at a could atea at a could ate a could atea at a could ate				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN						A-CIS- 22101	
CV Scoring Scale (CVSS)	e 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		Patch	NCIII	PCID
			specification exploration the denial condition that the definition of the denial condition of the denial condition the denial condition of the denial	Ppage loading page loading to the device, and to be device. D: CVE-	A succes allow the crease C resulting ce (DoS ich could elayed the					
firepower_thr	eat_defense									
Uncontrolled Resource Consumption	02-10-2019	7.8	Key E (IKEv Adapt (ASA) Firep (FTD) unaut attack an aff a den condi due to of sys could by sen traffic The a valid authe nor d addre staten applic of the explo attack memo	nerabilitics and an exploit and exploit an	version re of Cisc rity App re and Ci reat Def re could red, rem gger a re vice, res vice (Do e vulner rethis vuln rethis vuln dicious fected d loes not als to he VPN ttacker' to match he crypt ingress device. allow the haust sy urces, lee	obliance isco ense allow arote eload of sulting in attacker attacker erability. IKEv1 evice. need ession, a peer to map interfact An e estem ading to	n n er y N/A	A	A-CIS-1 22101	
CV Scoring Scal (CVSS)	e 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
			CVE ID : CVE-2019-15256		
Improper Input Validation	02-10-2019	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device. CVE ID: CVE-2019-12673	N/A	A-CIS-FIRE- 221019/51
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to	N/A	A-CIS-FIRE- 221019/52

3-4

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12674		
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675	N/A	A-CIS-FIRE- 221019/53
Improper Input Validation	02-10-2019	3.3	A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a	N/A	A-CIS-FIRE- 221019/54
CV Scoring Scal (CVSS)	e 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
			denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link- state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device. CVE ID: CVE-2019-12676		
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.	N/A	A-CIS-FIRE- 221019/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-12678		
Improper Input Validation	02-10-2019	7.2	A vulnerability in the command line interface (CLI) of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker with administrative privileges to execute commands on the underlying operating system with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by executing a specific CLI command that includes crafted arguments. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges. CVE ID: CVE-2019-12694	N/A	A-CIS-FIRE- 221019/56
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user- supplied input by the web- based management interface of an affected device. An attacker could exploit this	N/A	A-CIS-FIRE- 221019/57

3-4

4-5

5-6

6-7

8-9

9-10

7-8

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Puk	olish Dat	е	CVSS	Description & CVE ID		F	atch	NCIII	PC ID		
					user of crafted explosed attacked script the intacked brown	rability left the intended link. A lit could a code in terface of the code in the cod	erface to success allow th ecute ar the cont or allow cess sen d inform	o click a ful e bitrary text of the sitive nation. 2695				
Uncontrolled Resource Consumption	02-	10-201	9	7.8	A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device. CVE ID: CVE-2019-12698				ne N/A		A-CIS-1 22101	
Improper Input Validation	02-	10-201	9	7.2	CLI of and C Defen	ple vulno Cisco Fi isco Fire ise (FTD an auth	XOS Soft power ') Softwa	ware Threat re could	N/A		A-CIS-1 22101	
CV Scoring Scal (CVSS)	e	0-1	1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges. CVE ID: CVE-2019-12699 A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS CV Scoring Scale O1 12 23 34 45 56 67 78 89 910	Weakness	Publish Date	cvss		Descripti	on & CVE	ID	P	atch	NCIII	PC ID
Uncontrolled Resource Consumption Unconsumption Consumption Consump				on the system privil vulne insuff An att vulne CLI co explo attack on the privil	e underly m (OS) we eges. The rabilities cacker counderly eges.	ying ope vith root ese s are due put valid ould expl s by inclu ents to s es. A succe allow the ecute con ying OS v					
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Resource	02-10-2019	6.8	A vulnerability in the configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system							
	CV Scoring Scal (CVSS)	e <u>0-1</u>	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	·		ion & CV	E ID		Patch	NCIII	PC ID
			vulne needs the sy		the atta ser crede	cker entials o	n			
identity_serv	ices_engine								_	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	based Identicould unaut attack site so again based The v insuff suppl proce mana attack vulne user t succe the at arbitr conte access based	A vulnerability in the webbased guest portal of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a crosssite scripting (XSS) attack against a user of the webbased management interface. The vulnerability is due to insufficient validation of usersupplied input that is processed by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browserbased information. CVE ID: CVE-2019-12631		- N/:	A	A-CIS- 22101		
unity_connec	tion									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	A vulnerability in the web- based interface of multiple Cisco Unified Communications products could allow an unauthenticated, remote attacker to conduct a cross- site scripting (XSS) attack against a user of the web-			s N/	A	A-CIS- 22101		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

based interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker	
could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	
CVE ID : CVE-2019-12707	
1 02-10-2019 43 attacker to conduct a gross N/A	S-UNIT- 019/63
	9-10

Weakness	Publish Date	cvss	Descriptio	n & CVE ID	Р	atch	NCIII	PCID
			password of a t An attacker cou unauthorized a of the targeted	ld then take ctions on beha	lf			
			CVE ID : CVE-2	019-1915				
unified_conta	ct_center_exp	ress						
Improper Input Validation	02-10-2019	4.3	A vulnerability in Cisco Unified Contact Center Express (UCCX) Software could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. The vulnerability is due to insufficient input validation of some parameters that are passed to the web server of the affected system. An attacker could exploit this vulnerability by convincing a user to follow a malicious link or by intercepting a user request on an affected device. A successful exploit could allow the attacker to perform cross-site scripting attacks, web cache poisoning, access sensitive browser-based information, and similar exploits. CVE ID: CVE-2019-15259		f ne N/A		A-CIS-1 22101	
security_man	ager							
Deserializati on of Untrusted Data	02-10-2019	7.5	A vulnerability deserialization by Cisco Securit could allow an unauthenticate attacker to execumnate on a device. The vuln to insecure deserialization	function used ty Manager d, remote cute arbitrary in affected nerability is du	N/A		A-CIS-9 22101	
CV Scoring Scal (CVSS)	e 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
			user-supplied content by the affected software. An attacker could exploit this vulnerability by sending a malicious serialized Java object to a specific listener on an affected system. A successful exploit could allow the attacker to execute arbitrary commands on the device with the privileges of casuser.		
C			CVE ID : CVE-2019-12630		
firepower			M 14 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	I	
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	A-CIS-FIRE- 221019/66
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	A-CIS-FIRE- 221019/67
	ıt_database				

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	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-10-2019	5	A vulnerability in the file and malware inspection feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass the file and malware inspection policies on an affected system. The vulnerability exists because the affected software insufficiently validates incoming traffic. An attacker could exploit this vulnerability by sending a crafted HTTP request through an affected device. A successful exploit could allow the attacker to bypass the file and malware inspection policies and send malicious traffic through the affected device. CVE ID: CVE-2019-12701	N/A	A-CIS-VDB 221019/68
Cmsmadesim	ple				
cms_made_sii	mple				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	06-10-2019	3.5	CMS Made Simple (CMSMS) 2.2.11 allows XSS via the Site Admin > Module Manager > Search Term field. CVE ID : CVE-2019-17226	N/A	A-CMS- CMS 221019/69
Cpanel					
cpanel					
Insufficient Session Expiration	09-10-2019	6.5	cPanel before 82.0.15 allows API token credentials to persist after an account has been renamed or terminated (SEC-517).	N/A	A-CPA- CPAN- 221019/70
CV Scoring Scal (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		Descript	ion & CV	E ID		Patch	NCIII	PC ID
			CVE I	D : CVE-	2019-1	7375				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	4.3	cPanel before 82.0.15 allows self XSS in the SSL Certificate Upload interface (SEC-521). CVE ID: CVE-2019-17376					A	A-CPA CPAN- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	4.3	self X	el before SS in Liv ss (SEC-5 D : CVE-	eAPI exa 524).	ample	N/	A	A-CPA CPAN- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	4.3	cPanel before 82.0.15 allows self XSS in the SSL Key Delete interface (SEC-526). CVE ID: CVE-2019-17378				N/	A	A-CPA CPAN- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	4.3	cPanel before 82.0.15 allows self stored XSS in the WHM SSL Storage Manager interface (SEC-527). CVE ID: CVE-2019-17379				e N/	A	A-CPA CPAN- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	09-10-2019	4.3	cPanel before 82.0.15 allows self XSS in the WHM Update Preferences interface (SEC-528). CVE ID: CVE-2019-17380					A	A-CPA- CPAN- 221019/75	
CV Scoring Scal (CVSS)	e 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')					
Dell					
encryption					
Untrusted Search Path	07-10-2019	6.9	The vulnerability is limited to the installers of Dell Encryption Enterprise versions prior to 10.4.0 and Dell Endpoint Security Suite Enterprise versions prior to 2.4.0. This issue is exploitable only during the installation of the product by an administrator. A local authenticated low privileged user potentially could exploit this vulnerability by staging a malicious DLL in the search path of the installer prior to its execution by a local administrator. This would cause loading of the malicious DLL, which would allow the attacker to execute arbitrary code in the context of an administrator. CVE ID: CVE-2019-3745	N/A	A-DEL- ENCR- 221019/76
endpoint_sec	urity_suite_en	terpri	se		
Untrusted Search Path	07-10-2019	6.9	The vulnerability is limited to the installers of Dell Encryption Enterprise versions prior to 10.4.0 and Dell Endpoint Security Suite Enterprise versions prior to 2.4.0. This issue is exploitable only during the installation of the product by an administrator. A local authenticated low privileged user potentially could exploit	N/A	A-DEL- ENDP- 221019/77
CV Scoring Sca (CVSS)	le 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	NCII	PC ID
			this vulnerability by staging a malicious DLL in the search path of the installer prior to its execution by a local administrator. This would cause loading of the malicious DLL, which would allow the attacker to execute arbitrary code in the context of an administrator. CVE ID: CVE-2019-3745							
Elasticsearch										
kibana				1 63						
Incorrect Permission Assignment for Critical Resource	01-10-2019	3.5	A local file disclosure flaw was found in Elastic Code versions 7.3.0, 7.3.1, and 7.3.2. If a malicious code repository is imported into Code it is possible to read arbitrary files from the local filesystem of the Kibana instance running Code with the permission of the Kibana system user. CVE ID: CVE-2019-7618					A	A-ELA 22101	-KIBA- 9/78
eleopard										
animate_it\!										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	4.3	The animate-it plugin before 2.3.4 for WordPress has XSS. CVE ID: CVE-2019-17384					A	A-ELE ANIM- 22101	
Improper Neutralizatio n of Input During Web	09-10-2019	4.3	2.3.5	nimate-i for Word	lPress h	as XSS.	N/A	A	A-ELE ANIM- 22101	
CV Scoring Scal	e 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
Page Generation ('Cross-site Scripting')					
emlog					
emlog					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-10-2019	5.5	emlog through 6.0.0beta allows remote authenticated users to delete arbitrary files via admin/template.php?action=d el&tpl=/ directory traversal. CVE ID: CVE-2019-17073	N/A	A-EML- EMLO- 221019/81
enterprisedt					
completeftp_s	server				
Information Exposure Through Log Files	02-10-2019	3.5	EnterpriseDT CompleteFTP Server prior to version 12.1.3 is vulnerable to information exposure in the Bootstrap.log file. This allows an attacker to obtain the administrator password hash. CVE ID: CVE-2019-16116	N/A	A-ENT- COMP- 221019/82
etoilewebdes	ian		CVE ID . CVE-2019-10110		
	igii				
ultimate_faq	T		Eurotions /EWD HEAO Import		
Improper Input Validation	07-10-2019	5	Functions/EWD_UFAQ_Import. php in the ultimate-faqs plugin through 1.8.24 for WordPress allows unauthenticated options import. CVE ID: CVE-2019-17232	N/A	A-ETO-ULTI- 221019/83
Improper Neutralizatio n of Special Elements in Output Used	07-10-2019	4.3	Functions/EWD_UFAQ_Import. php in the ultimate-faqs plugin through 1.8.24 for WordPress allows HTML content injection. CVE ID: CVE-2019-17233	N/A	A-ETO-ULTI- 221019/84
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pub	lish Date	cvss		Description & CVE ID				Pa	atch	NCIII	PC ID
by a Downstream Component ('Injection')												
Exiv2												
exiv2												
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-1	10-2019	4.3	to trig Exiv2 when Exiv2 readI crwin there relation	0.27.2 a gger a cr ::getULo called fi ::Interna Directory nage_int is no val onship of fset and D: CVE-	ash in ong in ty com al::CiffDi o in cpp, bed lidation of the tot size.	pes.cpp rectory: cause of the al size to	N,	//A		A-EXI- 22101	
eyoucms												
eyoucms												
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-1	10-2019	4.3	has XI login. paran	Ems thro SS relate php web neter. D : CVE -	ed to the o_record	num		/A		A-EYO EYOU- 22101	
Facebook												
hhvm												
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-1	10-2019	7.5	when numb read/bound leadin execu	Insufficient boundary checks when formatting numbers in number_format allows read/write access to out-of-bounds memory, potentially leading to remote code execution. This issue affects HHVM versions prior to 3.30.10, all versions between			hu ac hv m a5 fd c2	https://git hub.com/f acebook/h hvm/com mit/dbeb9 a56a638e3 fdcef8b691 c2a296713 2dae692,		A-FAC- HHVM- 221019/87	
CV Scoring Scal (CVSS)	le	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		Descript	ion & CV	E ID		Patch	NCIII	PC ID
			betwee version 4.20.1 4.23.0	4.0.0 and 4.8.5, all versions between 4.9.0 and 4.18.2, and versions 4.19.0, 4.19.1, 4.20.0, 4.20.1, 4.20.2, 4.21.0, 4.22.0, 4.23.0. CVE ID: CVE-2019-11929				cps://hh a.com/bl /2019/0 25/secu y- date.htm cps://w v.facebo a.com/sec ty/advis es/cve- 19-		
fastadmin										
fastadmin										
Cross-Site Request Forgery (CSRF)	10-10-2019	6.8	fastad 1.0.0.2 a public /admi vulne	tue was of the land of the lan	05_beta. php/adr CSRF	There is	N /	A	A-FAS- 22101	
Fasterxml										
jackson-datal	oind									
Improper Input Validation	01-10-2019	7.5	was d jackso throu Typin global prope expos the se dbcp and an RMI s	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the commonsdbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make				A	A-FAS- 22101	•
CV Scoring Scal (CVSS)	e 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
			the service execute a malicious payload. This issue exists because of org.apache.commons.dbcp.dat asources.SharedPoolDataSour ce and org.apache.commons.dbcp.dat asources.PerUserPoolDataSou rce mishandling. CVE ID: CVE-2019-16942		
Improper Input Validation	01-10-2019	7.5	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy.P6DataS ource mishandling. CVE ID: CVE-2019-16943	N/A	A-FAS-JACK- 221019/90
Improper Input Validation	07-10-2019	7.5	A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLook up. CVE ID: CVE-2019-17267	N/A	A-FAS-JACK- 221019/91
fecmall					
fecmall					

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	Publish Date	CVSS		Descript	ion & CV	E ID	F	atch	NCIII	PC ID
Unrestricted Upload of File with Dangerous Type	04-10-2019	6.5	An unrestricted file upload vulnerability was discovered in catalog/productinfo/imageupl oad in Fecshop FecMall 2.3.4. An attacker can bypass a frontend restriction and upload PHP code to the webserver, by providing image data and the image/jpeg content type, with a .php extension. This occurs because the code relies on the getimagesize function. CVE ID: CVE-2019-17188						A-FEC- FECM- 22101	
Foxitsoftware										
foxit_studio_p	hoto									
Out-of- bounds Write	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8783.				N/A		A-FOX- 22101	
Out-of-	03-10-2019	6.8	This vulnerability allows			N/A		A-FOX	-FOXI-	
CV Scoring Scal (CVSS)	e 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 & CVI	ID .	P	atch	NCIII	PC ID
bounds Read			arbitrinstal Photo interaction walice exists TIFF for validate data, past to struct leverace executhe cut CAN-8		e on affects of Foxit S O9. User required allocated to the spectal properties of properties an allocattacker vulnerable to cocess. We have considered to the complete to			22101	9/94	
Out-of- bounds Read	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of				N/A		A-FOX- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	rrent pr 3-4	4-5	5-6	6-7	7-8	8-9	9-10

phantompdf This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656. CVE ID : CVE-2019-13315 This vulnerability allows remove A-FOX-PHAN-221019/96 A-FOX-PHAN-221019/96 A-FOX-PHAN-221019/96 A-FOX-PHAN-221019/96 A-FOX-PHAN-221019/96 A-FOX-PHAN-221019/96 A-FOX-PHAN-221019/97	Weakness	Publish Date	cvss	Description & CVE ID					Patch	NCIII	PC ID
Use After Free O4-10-2019 O4				CAN-89	22.						
This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656. CVE ID : CVE-2019-13315 This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this CV Scoring Scale O4-10-2019 6.8 This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this				CVE ID	: CVE-	2019-1	3325				
Use After Free Use After Free 04-10-2019 6.8 A-FOX- N/A A-FOX- N/A A-FOX- PHAN- 221019/97	phantompdf										
Use After Free O4-10-2019 6.8 O4-10-2019 O4-10-2019 CV Scoring Scale O5-10-2019 Temote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this CV Scoring Scale O4-10-2019 O4-10-2019 O4-10-2019 O4-10-2019 O4-10-2019 O4-10-2019 O5-10-2019 O5-		04-10-2019	6.8	remote atackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.					A	PHAN-	
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		04-10-2019	6.8	This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An				N/A	A	PHAN-	
	_	e 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute code in the context of the current process. Was ZDI-CAN-8757. CVE ID: CVE-2019-13316		
Use After Free	04-10-2019	6.8	This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759. CVE ID: CVE-2019-13317	N/A	A-FOX- PHAN- 221019/98
Use of Externally- Controlled Format String	04-10-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of the util.printf Javascript method. The application processes the %p parameter in the format string, allowing	N/A	A-FOX- PHAN- 221019/99
CV Scoring Scal (CVSS)	e 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
			heap addresses to be returned to the script. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8544. CVE ID: CVE-2019-13318		
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.	N/A	A-FOX- PHAN- 221019/100
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of	N/A	A-FOX- PHAN- 221019/101
CV Scoring Scal	e 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	Pat	ch	NCIIF	PC ID
			validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8814. CVE ID: CVE-2019-13320				
Improper Handling of Exceptional Conditions	02-10-2019	6.8	An exploitable memory corruption vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 9.4.1.16828. A specially crafted PDF document can trigger an out-of-memory condition which isn't handled properly, resulting in arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability. CVE ID: CVE-2019-5031	N/A		A-FOX- PHAN- 22101	
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deleteItemAt method when processing AcroForms. The issue results from the lack of validating the existence of an	N/A		A-FOX- PHAN- 22101	
CV Scoring Scal (CVSS)	e 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
			object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295. CVE ID: CVE-2019-6774		
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.	N/A	A-FOX- PHAN- 221019/104
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing	N/A	A-FOX- PHAN- 221019/105
CV Scoring Scal (CVSS)	le 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	ID .	Р	atch	NCIII	PC ID
			Acroffrom existed performs objected with a execution control of the cut of th	rmarks we forms. The lack ence of an ence of the code in the code in the code of the code of the ence of t	he issue of valida n object peration ncker can n conjui nerabili n the co					
reader			-				<u> </u>		T	
Use After Free	04-10-2019	6.8	remorarbitrinstal 9.5.0. is required vulne must open issue validate objection operation attack vulne in the	This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.					A-FOX READ- 22101	
Use After Free	04-10-2019	6.8	This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in						A-FOX READ- 22101	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CV	į į	Patch	NCII	PC ID	
			malicio malicio exists v Calcula results validat object operat attacke vulnera in the o	within thate action from the cing the prior to ions on er can lead ability to context of s. Was Z	e or ope The spe he hand ns. The existen perform the obje verage o execu- of the c	en a ecific flav elling of issue of ce of an ming ect. An this te code urrent I-8757.	W			
Use After Free	04-10-2019	6.8	This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759.						A-FOX READ- 22101	
Use of Externally- Controlled Format String	04-10-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.5.0.20723. User				N/A	1	A-FOX READ- 22101	
CV Scoring Scal (CVSS)	e 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	NCIIF	PC ID
			interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of the util.printf Javascript method. The application processes the %p parameter in the format string, allowing heap addresses to be returned to the script. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8544.				1			
			CVE I	D : CVE-	2019-1					
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.				N/A		A-FOX- READ- 22101	
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute			N/A		A-FOX- READ-	•	
CV Scoring Scal	e 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	atch	NCIII	PC ID
			arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8814.						22101	9/111
				D : CVE-						
Out-of- bounds Read	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8864.				N/A		A-FOX READ- 22101	9/112
Use After	03-10-2019	6.8	This vulnerability allows			N/A		A-FOX	-	
CV Scoring Scal (CVSS)	e 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
Free			remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8888.		READ- 221019/113
Use After Free	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8913.	N/A	A-FOX- READ- 221019/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13328		
Access of Resource Using Incompatible Type ('Type Confusion')	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can resul in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8695.	N/A	A-FOX- READ- 221019/115
Access of Resource Using Incompatible Type ('Type Confusion')	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG files. The issue results from the lack of proper validation of user-supplied data, which can resul in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8742.	N/A	A-FOX- READ- 221019/116
CV Scoring Scal (CVSS)	e 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
			CVE ID: CVE-2019-13330		
Out-of- bounds Read	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8838.	N/A	A-FOX- READ- 221019/117
Use After Free	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of templates in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of	N/A	A-FOX- READ- 221019/118

3-4

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Missing Release of Resource after Effective Lifetime	-2019	5	CAN-9 CVE II Foxit	D : CVE-		/as ZDI-				
Release of Resource after Effective	-2019	5	Foxit l			3332				
			if insu	keader t cess Viol officient t D : CVE-	memory	d crash exists.	S N/A		A-FOX- READ- 22101	
Improper Handling of Exceptional Conditions	-2019	6.8	An exploitable memory corruption vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 9.4.1.16828. A specially crafted PDF document can trigger an out-of-memory condition which isn't handled properly, resulting in arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability. CVE ID: CVE-2019-5031						A-FOX- READ- 22101	
Use After Free 04-10-	-2019	6.8	remote arbitratinstall 9.4.1.1 is required with the open a specific delete proces	rulnerabe attack ary code lations of 16828. Unired to rability in a malicidal fit of the strength of the stren	ers to execute on affect of Foxit Fo	cecute cted Reader raction chis ne target page or Γhe thin the when s. The			A-FOX- READ- 22101	
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	Pa	atch	NCIII	PC ID
			validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295. CVE ID: CVE-2019-6774				
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.	N/A		A-FOX READ- 22101	
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField	N/A		A-FOX READ- 22101	
CV Scoring Scal (CVSS)	e 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
			method when processing watermarks within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI- CAN-8801.
freerdp			CVE ID : CVE-2019-6776
•			
freerdp			
Missing Release of Resource after Effective Lifetime	04-10-2019	5	libfreerdp/codec/region.c in FreeRDP through 1.1.x and 2.x through 2.0.0-rc4 has memory leaks because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value. CVE ID: CVE-2019-17177
Missing Release of Resource after Effective Lifetime	04-10-2019	5	HuffmanTree_makeFromFrequ encies in lodepng.c in LodePNG through 2019-09-28, as used in WinPR in FreeRDP and other products, has a memory leak because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value. CVE ID : CVE-2019-17178
frostming			
redis_wrappe	er		
Deserializati on of	05-10-2019	7.5	Uncontrolled deserialization of a pickled object in models.py A-FRO-REDI- 221019/126
CV Scoring Sca (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		Descript	ion & CV	E ID		Pa	itch	NCIII	PC ID		
Untrusted Data			(aka R 0.3.0 a	st Ming Redis Wr allows a te arbitr	apper) ttackers	before to							
			CVE I	D : CVE-	2019-1	7206							
glyphandcog													
xpdfreader													
NULL Pointer Dereference	01-10-2019	4.3	NULL becau initial Catalo	Catalog.cc in Xpdf 4.02 has a NULL pointer dereference because Catalog.pageLabels is initialized too late in the Catalog constructor.				N/A		A-GLY 22101	-XPDF- 9/127		
Gnome													
libsoup													
Out-of- bounds Read	06-10-2019	7.5	until 2 buffer soup_ in sou prope messa proce	p from v. 2.68.1 ha r over-rentlm_pa p-auth-rly checurates age's lentled eding w. D: CVE-	ead beca rse_chal ntlm.c d k an NT gth befo ith a me	ap-based use llenge() oes not LM ore mcpy.		N/A		A-GNC 22101			
gonitro													
nitropdf													
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-10-2019	6.8	file en lead to when in Nits carefu this ca execu this vo would	A specifically crafted jpeg2000 file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.			embedded in a PDF file can I to a heap corruption en opening a PDF document I itroPDF 12.12.1.522. With eful memory manipulation, can lead to arbitrary code cution. In order to trigger vulnerability, the victim ald need to open the					A-GON NITR- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	-4 4-5 5-6			7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS		Descript	ion & CVI	E ID	F	atch	NCIII	PC ID								
			CVE I	D : CVE-	2019-5	045												
Out-of- bounds Write	09-10-2019	6.8	file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.				lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.				file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the				n nt n		A-GON NITR- 22101	
Use After Free	09-10-2019	6.8	An exploitable Use After Free vulnerability exists in the CharProcs parsing functionality of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a Use After Free. An attacker can craft a malicious PDF to trigger this vulnerability. CVE ID: CVE-2019-5047						A-GON NITR- 22101									
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-10-2019	6.8	A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file. CVE ID: CVE-2019-5048						A-GON NITR- 22101									
Improper Restriction of Operations	09-10-2019	6.8	A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful						A-GON NITR- 22101									
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3					7-8	8-9	9-10								

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID						
within the Bounds of a Memory Buffer			memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.								
			CVE ID: CVE-2019-5050								
Incorrect Type Conversion or Cast	09-10-2019	6.8	An exploitable use-after-free vulnerability exists in the Length parsing function of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a use-after-free condition. An attacker can craft a malicious PDF to trigger this vulnerability. CVE ID: CVE-2019-5053	N/A	A-GON- NITR- 221019/134						
HP											
arcsight_logg	er										
Unrestricted Upload of File with Dangerous Type	04-10-2019	6.5	Unrestricted file upload vulnerability in Micro Focus ArcSight Logger, version 6.7.0 and later. This vulnerability could allow Unrestricted Upload of File with Dangerous type. CVE ID: CVE-2019-11655	N/A	A-HP-ARCS- 221019/135						
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	04-10-2019	3.5	Stored XSS vulnerability in Micro Focus ArcSight Logger, affects versions prior to Logger 6.7.1 HotFix 6.7.1.8262.0. This vulnerability could allow Improper Neutralization of Input During Web Page Generation ('Crosssite Scripting'). CVE ID: CVE-2019-11656	N/A	A-HP-ARCS- 221019/136						
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10						

Weakness	Publish Dat	e CVSS		Descript	ion & CV	E ID	ı	Patch	NCIII	PC ID				
hrworks														
hrworks														
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	08-10-201	9 3.5	HRworks 3.36.9 allows XSS via the purpose of a travelexpense report. CVE ID: CVE-2019-16416						A-HRW HRWO 22101	-				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	08-10-201	9 3.5	XSS vi	HRworks FLOW 3.36.9 allows XSS via the purpose of a travelexpense report. CVE ID: CVE-2019-16417					A-HRW HRWO 22101	-				
IBM														
jazz_reportin	g_service													
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-201	9 3.5	(JRS) 6.0.4, vulne script allow arbitr the W intend poten crede truste ID: 16	IBM Jazz Reporting Service (JRS) 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6, and 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: 164115.				(JRS) 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6, and 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			http ww m/s /pa de/ 0	os://w .ibm.co support ges/no 107469	A-IBM 22101	•
Improper Neutralizatio n of Input During Web Page	01-10-201	9 3.5	IBM Jazz Reporting Service (JRS) 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6, and 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability				ww s m/s /pa	es://w .ibm.co support ges/no 107469	A-IBM-JAZZ- 221019/140					
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID								
Generation ('Cross-site Scripting')			arbitr the W intended potent creded trusted ID: 16	s users t cary Java ded func tially lea ntials dised session 4116.	Script cous alteri tionality ading to sclosure n. IBM X	ode in ng the within X-Force	а											
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-2019	3.5	(JRS) 6.0.4, vulne script allow arbitr the W intend poten crede truste ID: 16	azz Repo 6.0, 6.0.2 6.0.5, 6.0 rable to ing. This s users t ary Java deb UI th ded func tially lea ntials dis ed sessio 64118. D: CVE-	1, 6.0.2, 0.6, and cross-si vulner; o embed Script cous alteritionality ading to sclosure n. IBM \$	6.0.3, 6.0.6.1 i te ability d ode in ng the within	htt wv m/ /p/ de/	ps://w v.ibm.co support ages/no /107469	A-IBM 22101	•								
spectrum_sca	le																	
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	09-10-2019	7.2	been in IBM S through Spects through allow root p paran	A security vulnerability has been identified in all levels of IBM Spectrum Scale V5.0.0.0 through V5.0.3.2 and IBM Spectrum Scale V4.2.0.0 through V4.2.3.17 that could allow a local attacker to obtain root privilege by injecting parameters into setuid files. CVE ID: CVE-2019-4558				been identified in all levels of IBM Spectrum Scale V5.0.0.0 through V5.0.3.2 and IBM Spectrum Scale V4.2.0.0 through V4.2.3.17 that could allow a local attacker to obtain root privilege by injecting parameters into setuid files.				been identified in all levels of IBM Spectrum Scale V5.0.0.0 through V5.0.3.2 and IBM Spectrum Scale V4.2.0.0 through V4.2.3.17 that could allow a local attacker to obtain root privilege by injecting parameters into setuid files.				ps://w v.ibm.co support ages/no /107373	A-IBM 22101	
mq																		
Session Fixation	04-10-2019	7.5	IBM MQ 8.0.0.4 - 8.0.0.12, 9.0.0.0 - 9.0.0.6, 9.1.0.0 - 9.1.0.2, and 9.1.0 - 9.1.2 AMQP Listeners could allow an				wv m/	ps://w v.ibm.co 'support ages/no	A-IBM-MQ- 221019/143									
CV Scoring Scale (CVSS)	e 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		Pa	tch	NCIII	PC ID
			a sess client as the	thorized sion fixat s not be ey should 59352.	ion atta	ck due to onnected	0	e/88	36899		
			CVE I	D : CVE-	2019-4	227					
daeja_viewon	e										
Information Exposure	01-10-2019	5	5.0 th interi View used the sy 1595	rough 5 nal paran ONE clie in furthe ystem. IE 21.	ewONE Virtual .0.6 could expose meters to nts that could be er attacks against BM X-Force ID: https://w ww.ibm.c m/suppo /pages/n de/88438				om.co pport es/no	A-IBM- 22101	-
mavima anu	whore		CVE	D: CVE-	CVE-2019-4246						
maximo_anyv	viiere		IDM	Agrimo	A nyuuh o	ro 7.6.0					
Insecure Storage of Sensitive Information	10-10-2019	2.1	7.6.1, have which attack inform IBM X	IBM Maximo Anywhere 7.6.0, 7.6.1, 7.6.2, and 7.6.3 does not have device root detection which could result in an attacker gaining sensitive information about the device. IBM X-Force ID: 160198.				w.ib /su page	//w om.co pport es/no 07899	A-IBM- MAXI- 22101	
	J:		CVE	D : CVE-	2019-4	265					
security_guar	aium		IDM	·	C1:	0.0				T	
Improper Authenticati on	03-10-2019	6.5	9.5, a a priv could user t passv	BM Security Guardium 9.0, .5, and 10.6 are vulnerable to privilege escalation which ould allow an authenticated ser to change the accessmgr assword. IBM X-Force ID: 62768.			pr nt /s	https://su pportconte nt.ibm.com /support/p ages/node /957491		A-IBM- 22101	
			CVE I	D : CVE-	2019-4	422					
security_key_	lifecycle_ma	nager								ı	
Incorrect Authorizatio n	04-10-2019	5	IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 discloses sensitive information					221019/147			
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
			inforr moun syster 16513		an be us r attacks I-Force I		ges/no 302017			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	04-10-2019	4.3	IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 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. CVE ID: CVE-2019-4564					os://w .ibm.co support ges/no 302001	A-IBM- 22101	
security_dire	ctory_server								1	
Improper Restriction of Excessive Authenticati on Attempts	02-10-2019	5	6.4.0 accou could to bru	IBM Security Directory Server 6.4.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID:				os://w .ibm.co support ges/no 107704	A-IBM- 22101	
			CVE I	D : CVE-	2019-4	520				
URL Redirection to Untrusted Site ('Open Redirect')	02-10-2019	5.8	IBM Security Directory Server 6.4.0 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				http www. b m/s /pa de/	os://w .ibm.co support ges/no 107704	A-IBM- 22101	
CV Scoring Scal (CVSS)	e 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		
			the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 165660. CVE ID: CVE-2019-4538				
XML Injection (aka Blind XPath Injection)	02-10-2019	5.5	IBM Security Directory Server 6.4.0 does not properly neutralize special elements that are used in XML, allowing attackers to modify the syntax, content, or commands of the XML before it is processed by an end system. IBM X-Force ID: 165812. CVE ID: CVE-2019-4539	https://w ww.ibm.co m/support /pages/no de/107704	A-IBM-SECU- 221019/151		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	IBM Security Directory Server 6.4.0 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: 165815. CVE ID: CVE-2019-4542	https://w ww.ibm.co m/support /pages/no de/107704	A-IBM-SECU- 221019/152		
Insecure Storage of Sensitive Information	02-10-2019	5	IBM Security Directory Server 6.4.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 165951. CVE ID: CVE-2019-4549	https://w ww.ibm.co m/support /pages/no de/107704	A-IBM-SECU- 221019/153		
websphere_a							
Information	03-10-2019	5	IBM WebSphere Application	https://w	A-IBM-		
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		
Exposure Through an Error Message			Server 7.0, 8.0, 8.5, 9.0, and Liberty could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. IBM X-Force ID: 163177.				m /p	w.ibm. /suppo pages/r e/9590	ort 10	WEBS- 221019/154	
control dock			CVEI	CVE ID : CVE-2019-4441							
control_desk			IDMA	<i>x</i> :	Δ .					I	
Information Exposure Through an Error Message	09-10-2019	4	IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.				s w m /p	tps://w.ibm. /suppo pages/r e/1075	co ort 10	A-IBM- CONT- 221019/155	
			CVE ID : CVE-2019-4512								
maximo_asse	t_managemei	ıt									
Information Exposure Through an Error Message	09-10-2019	4	IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.					https://w ww.ibm.co m/support /pages/no de/107541 3		A-IBM- MAXI- 221019/156	
mavima for a	vistion		CVEI	D : CVE-	2019-4	512					
maximo_for_a	iviation		ID: C:		Δ -						
Information Exposure Through an Error Message	09-10-2019	4	IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554. CVE ID: CVE-2019-4512				s w m /p	etps://w.ibm. /suppo pages/r e/1075	co ort 10	A-IBM- MAXI- 221019/157	
maximo_for_l	ife_sciences										
Information 09-10-2019 4 Exposure			IBM Maximo Asset Management 7.6.1.1 generates					tps://v w.ibm.		A-IBM- MAXI-	
CV Scoring Scal (CVSS)	e 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		
Through an Error Message			an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554. CVE ID: CVE-2019-4512				/	/pag de/1	ipport es/no 07541	221019/158	
maximo_for_r	 nuclear_powe										
Information Exposure Through an Error Message	Exposure Through an 09-10-2019 Error		Mana an err sensit could attack IBM X	BM Maximo Asset Management 7.6.1.1 generates in error message that includes ensitive information that could be used in further attacks against the system. BM X-Force ID: 164554.				ww.i m/su /pag	s://w bm.co ipport es/no 07541	A-IBM- MAXI- 221019/159	
maximo_for_c	oil_and_gas		CVLI	D.CVL	2017 4	J12					
Information Exposure Through an Error Message	09-10-2019	4	Mana an err sensit could attack IBM X	IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554. CVE ID: CVE-2019-4512				ww.i m/su /pag	s://w bm.co ipport es/no 07541	A-IBM- MAXI- 221019/160	
maximo_for_t	ransportation	n									
Information Exposure Through an Error Message	are gh an 09-10-2019 4			IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554. CVE ID: CVE-2019-4512				ww.i m/su /pag	s://w bm.co apport es/no 07541	A-IBM- MAXI- 221019/161	
maximo_for_u	ıtilities										
Information Exposure Through an	09-10-2019	4	IBM Maximo Asset Management 7.6.1.1 generates an error message that includes			es v	ww.i	s://w bm.co ipport	A-IBM- MAXI- 221019/162		
CV Scoring Scal (CVSS)	e 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	on & CVE	ID	P	atch	NCIII	PC ID
Error Message			sensitive infori could be used i attacks against IBM X-Force ID	in furthe the syst D: 16455	er tem. 4.		es/no 07541		
			CVE ID : CVE-2	2019-45	512				
smartcloud_c	ontrol_desk								
Information Exposure Through an Error Message	09-10-2019	4	IBM Maximo A Management 7 an error messa sensitive informational be used in attacks against IBM X-Force ID CVE ID: CVE-2	7.6.1.1 geinge that is mation to furthe the system of the	includes hat er tem. 4.	ww.i m/si /pag	s://w bm.co upport es/no 07541	A-IBM SMAR- 22101	
tivoli intogra	tion compose	r	CVL ID . CVL 2	2017 +3	12				
tivoli_integra	uon_compose	Г				Į.		T	
Information Exposure Through an Error Message	09-10-2019	4	IBM Maximo A Management 7 an error messa sensitive infort could be used intacks against IBM X-Force ID	7.6.1.1 ge age that i mation t in furthe the syst	includes hat er tem.	ww.i m/si /pag	s://w bm.co upport es/no 07541	A-IBM 22101	
			CVE ID : CVE-2	2019-45	12				
intelliantech									
remote_acces	S								
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	07-10-2019	10	Intellian Remote Access 3.18 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the Ping Test field. CVE ID: CVE-2019-17269					A-INT- REMO 22101	-
Intelliants									
subrion									
Improper	06-10-2019	3.5	Subrion 4.2.1 allows XSS via N/A					A-INT-	SUBR-
CV Scoring Scal (CVSS)	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Da	ite CVSS	Description & CVE ID						tch	NCIII	PC ID
Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')			the panel/members/ Username, Full Name, or Email field, aka an "Admin Member JSON Update" issue. CVE ID: CVE-2019-17225							22101	9/166
Irfanview											
irfanview											
Out-of- bounds Write	08-10-20	19 4.6	Mode WSQ! 000d	/iew 4.5 Write A ReadWS 563. D : CVE -	V startii Q+0x00	ng at 000000	00 N	N/A		A-IRF- 22101	
Out-of- bounds Write	08-10-20	19 4.6	Mode WSQ! 0009	/iew 4.5 Write A ReadWS 66f. D : CVE -	V startii Q+0x00	ng at 000000	0 N	I/A		A-IRF- 22101	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-10-20	19 6.8	from contr JPEG_ 55.	Jiew 4.5 a Faultir ol Code l LS+0x00 D: CVE-	ig Addre Flow sta 000000	ess to rting at 000031	I N	N/A		A-IRF- 22101	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-10-20	19 6.8	IrfanView 4.53 allows Data from a Faulting Address to control Code Flow starting at JPEG_LS+0x0000000000001d 8a. CVE ID: CVE-2019-17244					I/A		A-IRF- 22101	
Out-of- bounds Write	08-10-20	4.6	Mode WSQ! 0004	View 4.5 Write A ReadWS 359. D : CVE -	V startii Q+0x00	ng at 000000	00 N	N/A		A-IRF- 22101	
CV Scoring Scal (CVSS)	e 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		Pa	atch	NCIII	PC ID
Out-of- bounds Write	08-10-2019	6.8	Mode	View 4.5 Write A ReadWS 58c.	V startii	ng at	00	N/A		A-IRF- 22101	
			CVE I	D : CVE-	2019-1	7246					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-10-2019	6.8	from control Addre JPEG_ a8.	View 4.55 a Faultin ol a subs ess starti LS+0x00 D: CVE-	ng Addre equent ng at 0000000	ess to Write		N/A		A-IRF- 22101	
Out-of- bounds Write	08-10-2019	6.8	Mode WSQ! 0002!		V startii Q+0x00	ng at 000000	00	N/A		A-IRF- 22101	
				D : CVE-							
Out-of- bounds Write	08-10-2019	6.8	Mode WSQ!	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000 000d57b.						A-IRF- 22101	
			CVE I	D : CVE-	2019-1	7249					
Out-of- bounds Write	08-10-2019	6.8	Mode	View 4.5 Write A ReadWS 2f5.	V startii	ng at	00	N/A		A-IRF- 22101	
			CVE I	D : CVE-	2019-1	7250					
Out-of- bounds Write	08-10-2019	6.8	IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!GetPlugInInfo+0x00 000000000007d43.				00	N/A		A-IRF- 22101	
			CVE ID : CVE-2019-17251								
Out-of- bounds Write	08-10-2019	6.8	IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!Read_BadPNG+0x0 0000000000000115. CVE ID: CVE-2019-17252					N/A		A-IRF- 22101	
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6					5-7	7-8	8-9	9-10
(CVSS)											

Weakness	Publish Date	CVSS	Description &	CVE ID	Pa	itch	NCIII	PC ID		
Out-of- bounds Write	08-10-2019	6.8	IrfanView 4.53 allo Mode Write AV sta JPEG_LS+0x00000 b8.	rting at	N/A		A-IRF- 22101			
			CVE ID : CVE-2019	9-17253						
Out-of- bounds Write	08-10-2019	6.8	IrfanView 4.53 allo from a Faulting Ad control a subseque Address starting at FORMATS!Read_Ba 0000000000000010	dress to ent Write t adPNG+0x0 1.	N/A		A-IRF- 22101			
			CVE ID : CVE-2019							
Out-of- bounds Write	08-10-2019	6.8	IrfanView 4.53 allo Mode Write AV sta EXR!ReadEXR+0x0 010836.	rting at	N/A		A-IRF- 22101			
			CVE ID : CVE-2019	9-17255						
Out-of- bounds Write	08-10-2019	6.8	IrfanView 4.53 allo Mode Write AV sta DPX!ReadDPX_W+ 000001203.	rting at	N/A		A-IRF- 22101			
			CVE ID : CVE-2019	9-17256						
Improper Check for Unusual or Exceptional	08-10-2019	4.3	IrfanView 4.53 allo Exception Handler Corrupted starting EXR!ReadEXR+0x0 02af80.	Chain to be	N/A		A-IRF- 22101			
Conditions			CVE ID : CVE-2019	9-17257						
Out-of- bounds Write	08-10-2019	6.8	IrfanView 4.53 allo from a Faulting Ad control a subseque Address starting at JPEG_LS+0x00000 9c.	dress to ent Write	N/A		A-IRF- 22101			
CVE ID : CVE-2019-17258										
Jenkins										
html_publish										
CV Scoring Scal	le 0-1	1-2	2-3 3-4 4-5	5 5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		Patch	NCIIF	PC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-2019	3.5	1.20 a the proname frame script explo change	ns HTML and earli coject an s in the l c, resulti ing vuln itable by ge those. D: CVE-	er did no d build of HTML re ng in a c erability ousers a	ot escape display eport ross-site v ble to	http kin urit ory 10- 01/	os://jen s.io/sec ty/advis /2019- /#SECU TY-1590	A-JEN- HTML- 22101	•
dingding										
Cleartext Storage of Sensitive Information	01-10-2019	2.1	stores in job Jenkin be vie Exten access systen	ns Dingd s creden config.x ns maste wed by ded Rea s to the n m.	tials une ml files r where users wi d permi master fi	encrypte on the they can ith ssion, or ile	kin urit ory 10- 01/	os://jen s.io/sec ty/advis //2019- /#SECU TY-1423	A-JEN- 22101	
ldap_email										
Cleartext Transmissio n of Sensitive Information	01-10-2019	5	transi crede of the config result	ns LDAP mits con ntials in global J guration ting in th D: CVE-	figured plain te enkins form, po	xt as par otentially osure.	kin urit ory 10- 01/	ps://jen s.io/sec ty/advis /2019- /#SECU TY-1515	A-JEN- 22101	
sourcegear_va	ault									
Cleartext Transmissio n of Sensitive Information	01-10-2019	5	Jenkins SourceGear Vault Plugin transmits configured credentials in plain text as part of job configuration forms, potentially resulting in their exposure. CVE ID: CVE-2019-10435					ps://jen s.io/sec ty/advis /2019- /#SECU TY-1524	A-JEN- 22101	
script_securit	T									
Improper	01-10-2019	6.5	A san	dbox by	pass		http	os://jen	A-JEN-	SCRI-
CV Scoring Scal (CVSS)	e 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
Control of Generation of Code ('Code Injection')			vulnerability in Jenkins Script Security Plugin 1.64 and earlier related to the handling of default parameter expressions in constructors allowed attackers to execute arbitrary code in sandboxed scripts. CVE ID: CVE-2019-10431	kins.io/sec urity/advis ory/2019- 10- 01/#SECU RITY-1579	221019/189
Jetbrains					
intellij_idea					
Missing Encryption of Sensitive Data	01-10-2019	4.3	JetBrains IntelliJ IDEA before 2019.2 was resolving the markdown plantuml artifact download link via a cleartext http connection. CVE ID: CVE-2019-14954	https://blo g.jetbrains. com/blog/ 2019/09/2 6/jetbrains -security- bulletin- q2-2019/	A-JET-INTE- 221019/190
upsource					
Information Exposure Through an Error Message	02-10-2019	5	Server metadata could be exposed because one of the error messages reflected the whole response back to the client in JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293. CVE ID: CVE-2019-12156	https://blo g.jetbrains. com/blog/ 2019/09/2 6/jetbrains -security- bulletin- q2-2019/	A-JET-UPSO- 221019/191
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	02-10-2019	10	In JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293, improper validation of user input for one of the fields could lead to Command Injection. CVE ID: CVE-2019-12157	N/A	A-JET-UPSO- 221019/192
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 78	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		Pa	atch	NCIIF	PC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-2019	4.3	2019. escap block XSS.	nins Upso 1.1412 v ing HTM commen D : CVE-	was not IL tags ii nts, lead	properly n a code ing to		N/A		A-JET- 22101	
teamcity											
Information Exposure Through an Error Message	02-10-2019	5	Server metadata could be exposed because one of the error messages reflected the whole response back to the client in JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293. CVE ID: CVE-2019-12156						s://blo orains. /blog/ 0/09/2 cbrains ority- etin- 019/	A-JET- TEAM- 22101	
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	02-10-2019	10	before version 1293, user i could Inject	In JetBrains TeamCity versions before 2018.2.5 and UpSource versions before 2018.2 build 1293, improper validation of user input for one of the fields could lead to Command Injection. CVE ID: CVE-2019-12157						A-JET- TEAM- 22101	
Information Exposure	01-10-2019	4	An issue was discovered in JetBrains TeamCity 2018.2.4. A TeamCity Project administrator could get access to potentially confidential server-level data. The issue was fixed in TeamCity 2018.2.5 and 2019.1. CVE ID: CVE-2019-15035					y 2018.2.4. A Id get access idential In he issue City 0.1.			9/196
Improper Neutralizatio n of Special	02-10-2019	9	An issue was discovered in JetBrains TeamCity 2018.2.4. A TeamCity Project					g.jetl	s://blo orains. /blog/	A-JET- TEAM- 22101	
CV Scoring Scal (CVSS)	e 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
Elements used in an OS Command ('OS Command Injection')			administrator could execute any command on the server machine. The issue was fixed in TeamCity 2018.2.5 and 2019.1. CVE ID: CVE-2019-15036	2019/09/2 6/jetbrains -security- bulletin- q2-2019/	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	An issue was discovered in JetBrains TeamCity 2018.2.4. It had several XSS vulnerabilities on the settings pages. The issues were fixed in TeamCity 2019.1. CVE ID: CVE-2019-15037	https://blo g.jetbrains. com/blog/ 2019/09/2 6/jetbrains -security- bulletin- q2-2019/	A-JET- TEAM- 221019/198
Improper Input Validation	01-10-2019	5	An issue was discovered in JetBrains TeamCity 2018.2.4. The TeamCity server was not using some security-related HTTP headers. The issue was fixed in TeamCity 2019.1. CVE ID: CVE-2019-15038	N/A	A-JET- TEAM- 221019/199
Improper Input Validation	01-10-2019	6.8	An issue was discovered in JetBrains TeamCity 2018.2.4. It had a possible remote code execution issue. This was fixed in TeamCity 2018.2.5 and 2019.1. CVE ID: CVE-2019-15039	https://blo g.jetbrains. com/blog/ 2019/09/2 6/jetbrains -security- bulletin- q2-2019/	A-JET- TEAM- 221019/200
Improper Certificate Validation	01-10-2019	5	An issue was discovered in JetBrains TeamCity 2018.2.4. It had no SSL certificate validation for some external https connections. This was fixed in TeamCity 2019.1. CVE ID: CVE-2019-15042	N/A	A-JET- TEAM- 221019/201
resharper	00.40.0046	4.4		DI / A	
Untrusted	02-10-2019	4.4	JetBrains ReSharper installers	N/A	A-JET-RESH-
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
Search Path)19.2 had rability.			22101	9/202
			CVE I	D : CVE-	2019-1	6407				
ktor										
Improper Input Validation	02-10-2019	7.5	JetBrains Ktor framework before 1.2.0-rc does not sanitize the username provided by the user for the LDAP protocol, leading to command injection. CVE ID: CVE-2019-12736					ps://blo etbrains. m/blog/ 19/09/2 etbrains curity- letin- 2019/	A-JET- 22101	
Use of Password Hash With Insufficient Computation al Effort	02-10-2019	5	UserHashedTableAuth in JetBrains Ktor framework before 1.2.0-rc uses a One-Way Hash with a Predictable Salt for storing user credentials. CVE ID: CVE-2019-12737					ps://blo etbrains. n/blog/ 19/09/2 etbrains curity- letin- 2019/	A-JET- 22101	
vim										
Insecure Storage of Sensitive Information	01-10-2019	5	before storing in the file. To synch access	_	n 0.52 w dual pro vim_setti file could to a pub Hub rep	ras oject data ings.xml d be olicly ository.	g.je cor 202 6/j -se bul	ps://blo etbrains. n/blog/ 19/09/2 etbrains curity- letin- 2019/	A-JET- 22101	
pycharm										
Uncontrolled Resource Consumption	02-10-2019	5	JetBrains PyCharm before 2019.2 was allocating a buffer of unknown size for one of the connection processes. In a very specific situation, it could lead to a remote invocation of an OOM error message because of Uncontrolled			g.je cor 201 d 6/j -se bul	ps://blo etbrains. n/blog/ 19/09/2 etbrains curity- letin- 2019/	A-JET- 22101		
CV Scoring Scal (CVSS)	e 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		Descript	ion & CV	E ID	ı	Patch	NCIII	PC ID
				ory Alloc						
			CVE I	D : CVE-	2019-1	4958				
toolbox									1	
Missing Encryption of Sensitive Data	02-10-2019	4.3	1.15.5 interr http c	ains Too 6605 wa nal URL v onnection	s resolvi via a clea on.	ing an artext	g.jet com 201 6/je -sec bull	os://blo cbrains. a/blog/ 9/09/2 etbrains curity- etin- 2019/	A-JET- 22101	
rider										
Untrusted Search Path	01-10-2019	4.6	2019. unsig JetBra ugin.I	nins Ride 1.2 was ned nins.Ride Repacked D : CVE-	using ar er.Unity. d.dll file	n Editor.P	N/A		A-JET- 22101	
hub										
Weak Password Recovery Mechanism for Forgotten Password	01-10-2019	5	earlie there user t and n policy	Brains H r than 2 was no o o chango o passw was im D: CVE-	018.4.11 option to e the part ord expiring plement	1436, o force a ssword iration ced.	N/A		A-JET- 22101	
youtrack										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-2019	4.3	JetBrains YouTrack versions before 2019.1.52584 had a possible XSS in the issue titles. CVE ID: CVE-2019-14952				g.jet com 201 6/je -sec bull	os://blo cbrains. a/blog/ 9/09/2 etbrains curity- etin- 2019/	A-JET- 22101	
Improper Neutralizatio	01-10-2019	4.3	JetBrains YouTrack versions before 2019.2.53938 had a				N/A	1	A-JET- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			possible XSS through issue attachments when using the Firefox browser. CVE ID: CVE-2019-14953		
Improper Preservation of Permissions	02-10-2019	4	JetBrains YouTrack before 2019.2.53938 was using incorrect settings, allowing a user without necessary permissions to get other project names. CVE ID: CVE-2019-14956	https://blo g.jetbrains. com/blog/ 2019/09/2 6/jetbrains -security- bulletin- q2-2019/	A-JET-YOUT- 221019/212
Cross-Site Request Forgery (CSRF)	02-10-2019	6.8	JetBrains YouTrack versions before 2019.1 had a CSRF vulnerability on the settings page. CVE ID: CVE-2019-15040	N/A	A-JET-YOUT- 221019/213
URL Redirection to Untrusted Site ('Open Redirect')	01-10-2019	5.8	JetBrains YouTrack versions before 2019.1.52545 allowed unbounded URL whitelisting because of Inclusion of Functionality from an Untrusted Control Sphere. CVE ID: CVE-2019-15041	N/A	A-JET-YOUT- 221019/214
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	In JetBrains YouTrack through 2019.2.56594, stored XSS was found on the issue page. CVE ID: CVE-2019-16171	N/A	A-JET-YOUT- 221019/215
jnoj	-				
jiangnan_onli	ine_judge			T	
Improper Neutralizatio	10-10-2019	4.3	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the	N/A	A-JNO-JIAN- 221019/216
CV Scoring Sca (CVSS)	le 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 of Input During Web Page Generation ('Cross-site Scripting')			Problem[title] parameter to web/polygon/problem/create or web/polygon/problem/updat e or web/admin/problem/create. CVE ID: CVE-2019-17489		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	4.3	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[description] parameter to web/admin/problem/create or web/polygon/problem/updat e. CVE ID: CVE-2019-17491	N/A	A-JNO-JIAN- 221019/217
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	4.3	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[sample_input] parameter to web/admin/problem/create or web/polygon/problem/updat e. CVE ID: CVE-2019-17493	N/A	A-JNO-JIAN- 221019/218
joomlashack					
shack_forms_	pro				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-10-2019	7.5	The Shack Forms Pro extension before 4.0.32 for Joomla! allows path traversal via a file attachment. CVE ID: CVE-2019-17399	N/A	A-JOO-SHAC- 221019/219
joyplus-cms_p	project				
joyplus-cms					

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	1-2	2-3	5	7	3-0	0-7	7-8	0-3	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-10-2019	5	joyplus-cms 1.6.0 allows manager/admin_pic.php?rootp ath= absolute path traversal. CVE ID: CVE-2019-17175	N/A	A-JOY-JOYP- 221019/220				
Kmplayer									
kmplayer									
Out-of- bounds Write	08-10-2019	4.6	KMPlayer 4.2.2.31 allows a User Mode Write AV starting at utils!src_new+0x000000000 14d6ee. CVE ID: CVE-2019-17259	N/A	A-KMP- KMPL- 221019/221				
koji_project									
koji									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-10-2019	4	Koji through 1.18.0 allows remote Directory Traversal, with resultant Privilege Escalation. CVE ID: CVE-2019-17109	https://do cs.pagure.o rg/koji/CV E-2019- 17109/, https://pa gure.io/koj i/commits /master	A-KOJ-KOJI- 221019/222				
kslabs									
ksweb									
Improper Control of Generation of Code ('Code Injection')	03-10-2019	6.5	The KSLABS KSWEB (aka ru.kslabs.ksweb) application 3.93 for Android allows authenticated remote code execution via a POST request to the AJAX handler with the configFile parameter set to the arbitrary file to be written to (and the config_text parameter	N/A	A-KSL- KSWE- 221019/223				
CV Scoring Scal (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	Pat	tch	NCIIPC ID				
			set to the content of the file to be created). This can be a PHP file that is written to in the public web directory and subsequently executed. The attacker must have network connectivity to the PHP server that is running on the Android device. CVE ID: CVE-2019-15766							
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-10-2019	4	KSLabs KSWEB 3.93 allows/ directory traversal, as demonstrated by the hostFile parameter. CVE ID: CVE-2019-16198	N/A		A-KSL- KSWE- 221019/224				
Kubernetes										
kube-state-m	etrics									
Information Exposure	03-10-2019	5	A security issue was discovered in kube-statemetrics 1.7.x before 1.7.2. An experimental feature was added to v1.7.0 and v1.7.1 that enabled annotations to be exposed as metrics. By default, kube-state-metrics metrics only expose metadata about Secrets. However, a combination of the default kubectl behavior and this new feature can cause the entire secret content to end up in metric labels, thus inadvertently exposing the secret content in metrics. CVE ID: CVE-2019-17110	N/A		A-KUB- KUBE- 221019/225				
laravel-admii	n									
CV Scoring Scal	le 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
laravel-admii	n				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	3.5	z-song laravel-admin 1.7.3 has XSS via the Slug or Name on the Roles screen, because of mishandling on the "Operation log" screen. CVE ID: CVE-2019-17433	N/A	A-LAR- LARA- 221019/226
lavalite					
lavalite					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	3.5	LavaLite through 5.7 has XSS via a crafted account name that is mishandled on the Manage Clients screen. CVE ID: CVE-2019-17434	N/A	A-LAV- LAVA- 221019/227
libfwsi_proje	ct				
libfwsi					
Out-of- bounds Read	06-10-2019	2.1	** DISPUTED ** In libyal libfwsi before 20191006, libfwsi_extension_block_copy_f rom_byte_stream in libfwsi_extension_block.c has a heap-based buffer over-read because rejection of an unsupported size only considers values less than 6, even though values of 6 and 7 are also unsupported. NOTE: the vendor has disputed this as described in the GitHub issue.	N/A	A-LIB-LIBF- 221019/228
			CVE ID : CVE-2019-17263		
liblnk_projec	t				
liblnk					

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	1-2	2-3	5	7	3-0	0-7	7-8	0-3	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	06-10-2019	variable name is used for a certain offset. NOTE: the vendor has disputed this as described in the GitHub issue. CVE ID: CVE-2019-17264 ** DISPUTED ** libyal liblnk		N/A	A-LIB-LIBL- 221019/229
Out-of- bounds Read	09-10-2019	2.1	** DISPUTED ** libyal liblnk 20191006 has a heap-based buffer over-read in the network_share_name_offset>2 0 code block of liblnk_location_information_re ad_data in liblnk_location_information.c, a different issue than CVE- 2019-17264. NOTE: the vendor has disputed this as described in the GitHub issue. CVE ID: CVE-2019-17401	N/A	A-LIB-LIBL- 221019/230
libpl_droidso	nroids gif pro	oiect	CVEID. CVE 2017 17101		
libpl_droidso					
Double Free	A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif before 1.2.15, as used in WhatsApp		https://w ww.facebo ok.com/sec urity/advis ories/cve- 2019- 11932	A-LIB-LIBP- 221019/231	
Libpng					

CV Scoring Scale	0-1	1_2	2-3	3-/1	1-5	5-6	6-7	7-8	2 _0	9-10
(CVSS)	0-1	1-2	2-3	3-4	4-3	3-0	0-7	7-0	0-3	3-10

Weakness	Publish Date	cvss	Descrip	tion & CV	E ID		Patch	NCIII	PC ID	
libpng										
Missing Release of Resource after Effective Lifetime	09-10-2019	4.3	libpng 1.6.37 leaks in png_ png_create_i: CVE ID : CVE	malloc_w nfo_struc	varn and t.	l N/	A	A-LIB- 22101		
Liferay										
liferay_portal	liferay_portal									
Deserializati on of Untrusted Data	04-10-2019	6.5	remote commoderate	Liferay Portal CE 6.2.5 allows remote command execution because of deserialization of a JSON payload. CVE ID: CVE-2019-16891				A-LIF- 22101		
Linuxmint										
mintinstall										
Deserializati on of Untrusted Data	02-10-2019	6.8	Manager) 7.9 allows code of REVIEWS_CA controlled by because an u	•				A-LIN- 22101		
lodev										
lodepngl										
Missing Release of Resource after Effective Lifetime	04-10-2019	5	HuffmanTree_makeFromFrequencies in lodepng.c in LodePNG through 2019-09-28, as used in WinPR in FreeRDP and other products, has a memory leak because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.			8, N/	A	A-LOD LODE- 22101		
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3 3-4	2-3 3-4 4-5 5-6			7-8	8-9	9-10	

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		Pat	ch	NCIII	PC ID
			CVE I	D : CVE-	2019-1	7178					
lqd											
liquid_speech	_balloon										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	4.3	LIQUI plugir allows Explo	D SPEE(n 1.0.5 fc s XSS wi rer.	eech-bal CH BALL or Word th Intern 2019-1	OON) Press net	xa N,	/A		A-LQD 22101	_
Matrixssl											
matrixssl											
Use of a Broken or Risky Cryptographi c Algorithm	03-10-2019	4.3	contain ECI gener or a remeasured hundred signing the proccurred scalar bit ler	ins a time DSA signeration. The content of the cont	nis allow ttacker, a luration housand tions, to y used.	e channe vs a loca able to of ls of comput The issu nath.c eaks the	l te e	/A		A-MATR- 22101	-
Metinfo											
metinfo											
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	10-10-2019	6.5	An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=language&c=language_general&a=doSearchParameter appno parameter, a different issue than CVE-2019-16997.			n N,	/A		A-MET METI- 22101		
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID		
			CVE I	D : CVE-	2019-1	7418						
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	10-10-2019	6.5	MetIninject admin &a=d paran	sue was an foot 7.0. To ion via to in/?n=us oGetUse neter. D: CVE-	There is S he er&c=ad rInfo id	SQL min_use	er N/A	A	A-MET METI- 22101			
Microfocus												
enterprise_de	enterprise_developer											
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	Enter Enter prior Upda Upda Patch vulne explo a mal	Reflected XSS on Micro Focus Enterprise Developer and Enterprise Server, all versions prior to version 3.0 Patch Update 20, version 4.0 Patch Update 12, and version 5.0 Patch Update 2. The vulnerability could be exploited to redirect a user to a malicious page or forge certain types of web requests.				A	A-MIC- ENTE- 22101			
enterprise_se	erver											
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	Enter Enter prior Upda Upda Patch vulne explo a mal certai	Reflected XSS on Micro Focus Enterprise Developer and Enterprise Server, all versions prior to version 3.0 Patch Update 20, version 4.0 Patch Update 12, and version 5.0 Patch Update 2. The vulnerability could be exploited to redirect a user to a malicious page or forge certain types of web requests. CVE ID: CVE-2019-11651			N/A	A	A-MIC- ENTE- 22101			
Microsoft												
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		Descript	ion & CV	E ID	F	atch	NCIIF	PC ID
excel_services	S									
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	vulne Micro the so handl 'Micro Execu CVE II 2019-	note code rability of soft Exconfitware for e objects cosoft Exconfit Excon	exists in el softw ails to p s in men cel Remo nerabili que from	are whe roperly nory, ak ote Code ty'. This CVE-	a N/A		A-MIC- 22101	
sql_server_ma	anagement_s	tudio								
Incorrect Permission Assignment for Critical Resource	10-10-2019	4	An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1376.						A-MIC- 22101	•
Incorrect Permission Assignment for Critical Resource	10-10-2019	4	An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1313. CVE ID: CVE-2019-1376						A-MIC- 22101	•
chakracore										
Improper Restriction of	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting					N/A		9/245
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1366.		
			CVE ID: CVE-2019-1307		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019- 1366. CVE ID: CVE-2019-1308	N/A	A-MIC- CHAK- 221019/246
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366. CVE ID: CVE-2019-1335	N/A	A-MIC- CHAK- 221019/247
Improper Restriction of Operations within the Bounds of a	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine	N/A	A-MIC- CHAK- 221019/248

3-4

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019- 1335. CVE ID: CVE-2019-1366		
edge			CVE 1D . CVE 2017 1300		
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357. CVE ID: CVE-2019-0608	N/A	A-MIC- EDGE- 221019/249
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019- 1366. CVE ID: CVE-2019-1307	N/A	A-MIC- EDGE- 221019/250
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366.	N/A	A-MIC- EDGE- 221019/251

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1308		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019- 1366. CVE ID: CVE-2019-1335	N/A	A-MIC- EDGE- 221019/252
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357	N/A	A-MIC- EDGE- 221019/253
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335. CVE ID: CVE-2019-1366	N/A	A-MIC- EDGE- 221019/254
office					
Improper Restriction of Operations within the	10-10-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka	N/A	A-MIC-OFFI- 221019/255
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pub	olish Date	CVSS		Descript	ion & CV	E ID		Pa	tch	NCIII	PC ID				
Bounds of a Memory Buffer				Execu CVE I	osoft Exc ition Vul D is unic 1327.	nerabili	ty'. This									
				CVE I	D : CVE-	2019-1	331									
office_365_pr	oplu	S														
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-	10-2019	9.3	vulne Micro the so handl 'Micro Execu CVE I	rability of soft Excorpt Excor	exists in el softw ails to p s in men cel Remo nerabili	are whe roperly nory, ak ote Code ty'. This	a N	N/A		A-MIC- 22101					
				CVE I	D : CVE-	2019-1	327					ļ				
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-	10-2019	9.3	vulne Micro the so handl 'Micro Execu CVE II	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE- 2019-1327. CVE ID: CVE-2019-1331						A-MIC- 22101					
internet_expl	orer							•								
Authenticati on Bypass by Spoofing	10-	10-2019	4.3	when not processed to the content of	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357. CVE ID: CVE-2019-0608				not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.			es	N/A		A-MIC- 22101	
Improper Restriction of	10-	10-2019	7.1	A remote code execution vulnerability exists in the way that the VBScript engine				y	N/A		A-MIC- 22101					
CV Scoring Scal (CVSS)	e	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		Pa	tch	NCIII	PC ID				
Operations within the Bounds of a Memory Buffer			aka 'V Execu CVE II	es objec BScript tion Vul D is unic 1239.	Remote nerabili	Code ty'. This	5								
			CVE I	D : CVE-	2019-1	238									
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	vulne that thandl aka 'V Execu CVE II 2019-	hat the VBScript engine andles objects in memory, ka 'VBScript Remote Code Execution Vulnerability'. This EVE ID is unique from CVE-2019-1238.				vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1238. CVE ID: CVE-2019-1239			N	N/A		A-MIC- 22101	
Authenticati on Bypass by Spoofing	10-10-2019	4.3	when improcookie Brows Vulne uniqu	ofing vu Microso perly ha es, aka 'I ser Spoo rability' e from (D : CVE-	oft Brow andle br Microsof ofing . This CV CVE-201	sers owser ft /E ID is 9-0608.	1	N/A		A-MIC- 22101					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	4.3	LIQUI plugir allow Explo	The liquid-speech-balloon (aka LIQUID SPEECH BALLOON) plugin 1.0.5 for WordPress allows XSS with Internet Explorer. CVE ID: CVE-2019-17070						A-MIC- 22101					
sharepoint_se	erver														
Improper Restriction of Operations within the Bounds of a Memory	10-10-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This					N/A		A-MIC- SHAR- 22101					
CV Scoring Scal (CVSS)	e 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
Buffer			CVE ID is unique from CVE-2019-1327.		
			CVE ID : CVE-2019-1331		
sharepoint_e	ntarnrica cars	zor	CVE ID . CVE-2019-1331		
snarepoint_cr	liter prise_serv	/CI	A cross-site-scripting (XSS)		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	3.5	vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. CVE ID: CVE-2019-1070	N/A	A-MIC- SHAR- 221019/264
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. CVE ID: CVE-2019-1328	N/A	A-MIC- SHAR- 221019/265
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	3.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1330. CVE ID: CVE-2019-1329	N/A	A-MIC- SHAR- 221019/266
Improper Privilege Management	10-10-2019	4	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint	N/A	A-MIC- SHAR- 221019/267

3-4

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publi	ish Date	CVSS		Descript	ion & CV	E ID		Pa	tch	NCIIF	PC ID
				Vulne	tion of P rability' e from (. This CV						
				CVE I	D : CVE-	2019-1	330					
office_online_	serve	r										
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10	0-2019	9.3	vulne Micro the so handl 'Micro Execu CVE II 2019-	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327. CVE ID: CVE-2019-1331						A-MIC- 22101	
sharepoint_fo	undat	tion		GVET	CVE ID : CVE-2019-1331							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10	0-2019	3.5	when Serve saniti reque Share 'Micro Vulne	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. CVE ID: CVE-2019-1328						A-MIC- SHAR- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')		0-2019	3.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1330. CVE ID: CVE-2019-1329					I/A		A-MIC- SHAR- 22101	
Improper		0-2019	4	An elevation of privilege			N	I/A		A-MIC-		
CV Scoring Scal (CVSS)	е	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
Privilege Management			vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1329.		SHAR- 221019/271
1			CVE ID : CVE-2019-1330		
excel			A manuska as da susankian		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1331.	N/A	A-MIC-EXCE- 221019/272
			CVE ID : CVE-2019-1327		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE- 2019-1327. CVE ID: CVE-2019-1331	N/A	A-MIC-EXCE- 221019/273
open_enclave	_software_de	velopm	ent_kit		
Information Exposure	10-10-2019	5	An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory, aka 'Open Enclave SDK Information Disclosure Vulnerability'. CVE ID: CVE-2019-1369	N/A	A-MIC- OPEN- 221019/274
Mozilla					
CV Scoring Scal (CVSS)	e 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		Patch	NCIIF	NCIIPC ID	
firefox											
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-2019	4.3	before possil attach Firefo	nins You' e 2019.2 ole XSS t nments v ox brows D : CVE-	53938 hrough when usi	had a issue ng the	N/A	1	A-MOZ FIRE- 22101		
mpc-hc											
mpc-hc											
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-10-2019	4.6	a Read Block mpc_l 00000	MPC-HC through 1.7.13 allows a Read Access Violation on a Block Data Move starting at mpc_hc!memcpy+0x00000000 0000004e. CVE ID: CVE-2019-17260				1	A-MPC - 22101		
netreo											
omnicenter											
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	09-10-2019	5	12.1.1 SQL In Blind paran name a GET allow sensit datab	Netreo OmniCenter through 12.1.1 allows unauthenticated SQL Injection (Boolean Based Blind) in the redirect parameters and parameter name of the login page through a GET request. The injection allows an attacker to read sensitive information from the database used by the application.				4	A-NET OMNI- 22101		
Nlnetlabs											
unbound											
Improper Restriction of	03-10-2019	5	Unbound before 1.9.4 accesses uninitialized memory, which allows remote attackers to				s N/A	1	A-NLN UNBO-		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	e CVSS		Descript	ion & CV	E ID		Pa	itch	NCIII	PC ID
Operations within the Bounds of a Memory			NOTI addre	er a crasl FY query ess of the n an acce	7. The so	ource IP nust				22101	9/278
Buffer			CVE I	D : CVE-	2019-1	6866					
online_store_s	system_pro	ject									
online_store_s	online_store_system										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-2019	9 3.5	v1.0, s user_v adida is not	rability Stored X view.php s_memb sanitize D : CVE -	SS in o where er_user d.	variable	e l	N/A		A-ONL ONLI- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-201	9 3.5	Vulnerability in Online Store v1.0, stored XSS in admin/user_view.php adidas_member_email variable CVE ID : CVE-2019-8289					N/A		A-ONL ONLI- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	01-10-201	9 4.3	Vulnerability in Online Store v1.0, The registration form requirements for the member email format can be bypassed by posting directly to sent_register.php allowing special characters to be included and an XSS payload to be injected. CVE ID: CVE-2019-8290					N/A		A-ONL ONLI- 22101	
Improper Limitation of a Pathname to a Restricted Directory	01-10-201	9 6.4	Online Store System v1.0 delete_file.php doesn't check to see if a user has administrative rights nor does it check for path traversal.					N/A		A-ONL ONLI- 22101	
CV Scoring Scal (CVSS)	e 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	atch	NCIII	PC ID
('Path Traversal')			CVE I	D : CVE-	2019-8	291				
Missing Authenticati on for Critical Function	01-10-2019	6.4	delete check authte admir arbitr	e Store S e_producto see if enticated nistrative ary prod D: CVE-	et.php do a user d or has e rights duct dele	oesn't allowing etion.	N/A		A-ONLI- ONLI- 22101	
Open-emr										
openemr										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	04-10-2019	4.3	XSS in library/custom_template/add_template.php in OpenEMR through 5.0.2 allows a malicious user to execute code in the context of a victim's browser via a crafted list_id query parameter. CVE ID: CVE-2019-17179						A-OPE OPEN- 22101	
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	05-10-2019	7.5	SQL Indemo	OpenEMR through 5.0.2 has SQL Injection in the Lifestyle demographic filter criteria in library/clinical_rules.php that affects library/patient.inc. CVE ID: CVE-2019-17197					A-OPE OPEN- 22101	
openmpt										
libopenmpt										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-10-2019	7.5	and 0 ModP and M libope restri	openmpt 4.x befo lug_Inst lodPlug_ enmpt_n ct the lead	re 0.4.9, rument! Sample! nodplug. ngths of	Name Name in c do not			A-OPE 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
			_	s in the er overf	•	ading to)			
						- 440				
			CVEI	D : CVE-	2019-1	7113				
openproject										
openproject										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	4.3	list in and 1 remote arbitr via th becau misha	An XSS vulnerability in project list in OpenProject before 9.0.4 and 10.x before 10.0.2 allows remote attackers to inject arbitrary web script or HTML via the sortBy parameter because error messages are mishandled. CVE ID: CVE-2019-17092				ttps://w w.openpr ect.org/r ease- otes/ope oroject- 0-0-2/, ttps://w w.openpr ect.org/r ease- otes/ope oroject-9-	A-OPE OPEN- 22101	
otcms										
otcms										
Improper Input Validation	09-10-2019	6.5	PHP (admir block SELE(not bl manir attack	IS v3.85 Gode Exends SysChes Into o CT stater ock the oulation cer can c D: CVE-	cution beckFile_outfile" ir ment, bu "into/** Thereforeate a .	pecause deal.php a a t does /outfile ore, the php file.	N,	/A	A-OTC OTCM- 22101	
Pbootcms										
Pbootcms										
Improper Neutralizatio n of Input During Web Page Generation	10-10-2019	3.5	PbootCMS 2.0.2 allows XSS via vectors involving the Pboot/admin.php?p=/Single/ ndex/mcode/1 and Pboot/?contact/ URIs.					/A	A-PBO PBOO- 22101	
CV Scoring Scal (CVSS)	e 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	NCIII	PC ID						
('Cross-site			CVE I	D : CVE-	2019-1	7417										
Scripting')																
pcprotect																
antivirus									T							
Improper Privilege Management	07-10-2019	7.2	instal %PRO Prote permit full per to the and it the pr called runs a allow privil AUTH substi	Is by def OGRAMF ct with v ssions, g ermissio content s subfol	ault to ILES(X8 very wea granting n "Every s of the ders. In a nstalls a yService System." er to esc NT SYSTEM ne servic	This ralate "by ce's norse.	er)" y		A-PCP- 22101							
pi-hole																
pi-hole																
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	09-10-2019	6.8	Inject	Pi-Hole 4.3 allows Command Injection. CVE ID : CVE-2019-13051		N/A		A-PII 22101								
Pivotal																
apps_manage	r		1				1.		1							
Incorrect Permission Assignment for Critical	01-10-2019	4	Pivotal Application Manager, versions 666.0.x prior to 666.0.36, versions 667.0.x prior to 667.0.22, versions			versions 666.0.x prior to 666.0.36, versions 667.0.x			versions 666.0.x prior to 666.0.36, versions 667.0.x			versions 666.0.x prior to 666.0.36, versions 667.0.x		s://piv io/sec y/cve- 9-	A-PIV- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5					9-10						

Weakness	Publi	sh Date	cvss		Description & CVE ID		F	atch	NCIII	PC ID	
Resource				version 669.0 prior vulne auther an approximation of the man possil report privil	.x prior ons 66913, and to 670.0 rability on ticated p with a rogram on that reege.	O.x prior version .7, conta where a user can name su can inter gets exe user can access to quires a	to s 670.0.2 nin a remote n create uch that pret into ecuted. n o a usago higher	a o	75		
pivotal_softwa	are										
pivotal_application_service											
Incorrect Permission Assignment for Critical Resource	01-10	0-2019	4	version 666.0 prior 668.0 prior vulne auther an approximate of the possible report privil	Pivotal Application Manager, versions 666.0.x prior to 666.0.36, versions 667.0.x prior to 667.0.22, versions 668.0.x prior to 668.0.21, versions 669.0.x prior to 669.0.13, and versions 670.0.x prior to 670.0.7, contain a vulnerability where a remote authenticated user can create an app with a name such that a csv program can interpret into a formula and gets executed. The malicious user can possibly gain access to a usage report that requires a higher privilege. CVE ID: CVE-2019-11275			http otal urit; 201 112		A-PIV- 22101	
Putty											
putty											
Allocation of Resources 01-10-2019 Without		7.5	PuTTY before 0.73 on Windows improperly opens port-forwarding listening			N/A	N/A		A-PUT- PUTT-		
CV Scoring Scal (CVSS)	е	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					
Limits or Throttling			sockets, which allows attackers to listen on the same port to steal an incoming connection.	221019/294					
T			CVE ID : CVE-2019-17067						
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	01-10-2019	5	PuTTY before 0.73 mishandles the "bracketed paste mode" protection mechanism, which may allow a session to be affected by malicious clipboard content. CVE ID: CVE-2019-17068	A-PUT- PUTT- 221019/295					
Improper Input Validation	01-10-2019	5	PuTTY before 0.73 might allow remote SSH-1 servers to cause a denial of service by accessing freed memory locations via an SSH1_MSG_DISCONNECT message. CVE ID: CVE-2019-17069	A-PUT- PUTT- 221019/296					
Python CVE 2013 17003									
pillow									
Allocation of Resources Without Limits or Throttling	04-10-2019	4.3	An issue was discovered in Pillow before 6.2.0. When reading specially crafted invalid image files, the library can either allocate very large amounts of memory or take an extremely long period of time to process the image. CVE ID: CVE-2019-16865	A-PYT-PILL- 221019/297					
realbigplugins									
client_dash									
Improper Neutralizatio n of Input During Web	alizatio 10-10-2019		The client-dash (aka Client Dash) plugin 2.1.4 for WordPress allows XSS.	A-REA-CLIE- 221019/298					
CV Scoring Scal	e 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			
Page Generation ('Cross-site Scripting')			CVE ID : CVE-2019-17071					
Redhat jboss_operations_network								
Use of Externally- Controlled Input to Select Classes or Code ('Unsafe Reflection')	03-10-2019	6.8	It was found that the fix for CVE-2014-0114 had been reverted in JBoss Operations Network 3 (JON). This flaw allows attackers to manipulate ClassLoader properties on a vulnerable server. Exploits that have been published rely on ClassLoader properties that are exposed such as those in JON 3. Additional information can be found in the Red Hat Knowledgebase article: https://access.redhat.com/site/solutions/869353. Note that while multiple products released patches for the original CVE-2014-0114 flaw, the reversion described by this CVE-2019-3834 flaw only occurred in JON 3. CVE ID: CVE-2019-3834	https://bu gzilla.redh at.com/sho w_bug.cgi?i d=CVE- 2019-3834	A-RED-JBOS- 221019/299			
jboss_enterpi	rise_applicatio	on_piat		T	<u> </u>			
Deserializati on of Untrusted Data	01-10-2019	7.5	A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes CVE-2017-17485, CVE-2017-7525, CVE-2017-15095, CVE-2018-5968, CVE-2018-7489, CVE-2018-1000873, CVE-2019-12086 reported for FasterXML	https://bu gzilla.redh at.com/sho w_bug.cgi?i d=CVE- 2019- 10202	A-RED-JBOS- 221019/300			
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9								

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			jackson-databind by implementing a whitelist approach that will mitigate these vulnerabilities and future ones alike. CVE ID: CVE-2019-10202		
single_sign-or	1				
Information Exposure Through Log Files	02-10-2019	4.3	A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files. CVE ID: CVE-2019-10212	https://bu gzilla.redh at.com/sho w_bug.cgi?i d=CVE- 2019- 10212	A-RED-SING- 221019/301
undertow					
Information Exposure Through Log Files	02-10-2019	4.3	A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files. CVE ID: CVE-2019-10212	https://bu gzilla.redh at.com/sho w_bug.cgi?i d=CVE- 2019- 10212	A-RED- UNDE- 221019/302
jboss_data_gr	id				
Information Exposure Through Log Files	02-10-2019	4.3	A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files. CVE ID: CVE-2019-10212	https://bu gzilla.redh at.com/sho w_bug.cgi?i d=CVE- 2019- 10212	A-RED-JBOS- 221019/303
jboss_fuse					

Weakness	Publish Date	cvss		Descript	ion & CV	E ID	P	atch	NCIII	PC ID
Information Exposure Through Log Files	02-10-2019	4.3	A flaw was found in, all under 2.0.20, in the Undertow DEBUG log for io.undertow.request.security. If enabled, an attacker could abuse this flaw to obtain the user's credentials from the log files. CVE ID: CVE-2019-10212					s://bu a.redh om/sho ug.cgi?i VE- 9-	A-RED 22101	-
Redmine										
redmine										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	10-10-2019	4.3	In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors. CVE ID: CVE-2019-17427				N/A		A-RED REDM- 22101	-
rpyc_project										
rpyc										
Missing Authorizatio n	03-10-2019	5	remo dynar attrib remo execu servic config	yC 4.1.x te attack mically mutes to cote proceetes code ce with deguration D: CVE-	er can nodify of construct dure cal for an F efault settings	bject t a I that RPyC	N/A		A-RPY- RPYC- 22101	
salesagility							·			
suitecrm										
Server-Side Request Forgery (SSRF)	02-10-2019	7.5	SalesAgility SuiteCRM 7.10.x 7.10.19 and 7.11.x before and 7.11.7 has SSRF. CVE ID: CVE-2019-13335				cs.su .com n/re /7.1	s://do nitecrm n/admi eleases 0.x/#_ 0_20,	A-SAL-SUIT- 221019/307	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
							cs.s .com n/r /7.7 7_1 http cs.s .com n/r /7.7	os://do uitecrm m/admi eleases 11.x/#_ 1_7, os://do uitecrm m/admi eleases 11.x/#_ 1_8		
Improper Privilege Management	02-10-2019	7.5	befor vulne escala		and 7.10 vertical	0.20 is privileg	cs.s .com n/r /7.1 http cs.s .com n/r /7.1	os://do uitecrm m/admi eleases 10.x/#_ 0_20, os://do uitecrm m/admi eleases 11.x/#_ 1_8	A-SAL- 22101	
SAP										
netweaver_pr	ocess_integr	ation								
Missing Authorizatio n	08-10-2019	4	Integrated before does author author the incontegrated Author Author	SAP NetWeaver Process Integration (B2B Toolkit), before versions 1.0 and 2.0, does not perform necessary authorization checks for an authenticated user, allowing the import of B2B table content that leads to Missing Authorization Check. CVE ID: CVE-2019-0367				os://wi cn.sap.c /wiki/p s/view ge.action geId=5	A-SAP- NETW 22101	-
businessobje	cts_business_	intelli	gence_p	olatform	1					
Improper Neutralizatio	08-10-2019	3.5		SAP BusinessObjects Business h Intelligence Platform (Web k					A-SAP- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	·					Patch	NCIII	PC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the chart title resulting in reflected Cross-Site Scripting CVE ID: CVE-2019-0374					/wiki/p s/view e.action geId=5 23050		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	08-10-2019	3.5	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the export dialog box of the report name resulting in reflected Cross-Site Scripting. CVE ID: CVE-2019-0375					os://wi cn.sap.c /wiki/p s/view e.action geId=5 .23050	A-SAP- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	08-10-2019	3.5	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows an attacker to save malicious scripts in the publication name, which can be executed later by the victim, resulting in Stored Cross-Site Scripting. CVE ID: CVE-2019-0376				http ki.s om, age pag ?pa ?pa	os://wi cn.sap.c /wiki/p s/view e.action geId=5 .23050	A-SAP- 22101	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	08-10-2019	3.5	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2, does not sufficiently encode user- controlled inputs and allows an attacker to store malicious				ki.s om age pag ?pa	os://wi cn.sap.c /wiki/p s/view e.action geId=5 .23050	A-SAP- 22101	
CV Scoring Scal (CVSS)	e 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')			scripts in the input controls, resulting in Stored Cross-Site Scripting. CVE ID: CVE-2019-0377		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	08-10-2019	3.5	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before version 4.2, does not sufficiently encode usercontrolled inputs and allows an attacker to store malicious scripts in the file name of the background image resulting in Stored Cross-Site Scripting. CVE ID: CVE-2019-0378	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050	A-SAP-BUSI- 221019/314
financial_cons	solidation				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	08-10-2019	3.5	SAP Financial Consolidation, before versions 10.0 and 10.1, does not sufficiently encode user-controlled inputs, which allows an attacker to execute scripts by uploading files containing malicious scripts, leading to reflected cross site scripting vulnerability. CVE ID: CVE-2019-0369	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050	A-SAP-FINA- 221019/315
XML Injection (aka Blind XPath Injection)	08-10-2019	6.4	Due to missing input validation, SAP Financial Consolidation, before versions 10.0 and 10.1, enables an attacker to use crafted input to interfere with the structure of the surrounding query leading to XPath Injection. CVE ID: CVE-2019-0370	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050	A-SAP-FINA- 221019/316
S-cms				1	
S-cms					

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	Publish Date	CVSS	Description & CVE ID					Patch	NCIII	PC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	4.3	via th memb from	S v1.5 ha e per/men paramet D : CVE -	nber_log er.	n.php N/A			S-CM- 9/317	
signal										
signal_private	e_messenger									
Improper Input Validation	05-10-2019	7.5	** DISPUTED ** The WebRTC component in the Signal Private Messenger application through 4.47.7 for Android processes videoconferencing RTP packets before a callee chooses to answer a call, which might make it easier for remote attackers to cause a denial of service or possibly have unspecified other impact via malformed packets. NOTE: the vendor plans to continue this behavior for performance reasons unless a WebRTC design change occurs. CVE ID: CVE-2019-17192				r N/ t	'A	A-SIG- 22101	
private_mess	enger									
Improper Input Validation	05-10-2019	5	The Signal Private Messenger application before 4.47.7 for Android allows a caller to force a call to be answered, without callee user interaction, via a connect message. The existence of the call is noticeable to the callee; however, the audio channel may be open before the callee can block eavesdropping.				n, N/	'A	A-SIG- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descripti	ion & CV	E ID	Р	atch	NCII	PC ID
			CVE I	D : CVE-	2019-1	7191				
sitos										
sitos_six										
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	07-10-2019	10	SITOS six Build v6.2.1 allows an attacker to inject arbitrary PHP commands. As a result, an attacker can compromise the running server and execute system commands in the context of the web user. CVE ID: CVE-2019-15746						A-SIT- 22101	SITO- 9/320
Improper Privilege Management	07-10-2019	6.5	SITOS six Build v6.2.1 allows a user with the user role of Seminar Coordinator to escalate their permission to the Systemadministrator role due to insufficient checks on the server side. CVE ID: CVE-2019-15747						A-SIT- 22101	SITO- 9/321
Unrestricted Upload of File with Dangerous Type	07-10-2019	7.5	SITOS six Build v6.2.1 permits unauthorised users to upload and import a SCORM 2004 package by browsing directly to affected pages. An unauthenticated attacker could use the upload and import functionality to import a malicious SCORM package that includes a PHP file, which could execute arbitrary PHP code. CVE ID: CVE-2019-15748				N/A		A-SIT- 22101	SITO- 9/322
Weak Password Recovery Mechanism for Forgotten	07-10-2019	4.3	SITOS six Build v6.2.1 allows a user to change their password and recovery email address without requiring them to confirm the change with their old password. This would				l N/A		A-SIT- 22101	SITO- 9/323
CV Scoring Scal (CVSS)	e 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
Password			allow an attacker with access to the victim's account (e.g., via XSS or an unattended workstation) to change that password and address.		
			CVE ID : CVE-2019-15749		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	07-10-2019	4.3	A Cross-Site Scripting (XSS) vulnerability in the blog function in SITOS six Build v6.2.1 allows remote attackers to inject arbitrary web script or HTML via the id parameter. CVE ID: CVE-2019-15750	N/A	A-SIT-SITO- 221019/324
Unrestricted Upload of File with Dangerous Type	07-10-2019	10	An unrestricted file upload vulnerability in SITOS six Build v6.2.1 allows remote attackers to execute arbitrary code by uploading a SCORM file with an executable extension. This allows an unauthenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to the web root of the application. CVE ID: CVE-2019-15751	N/A	A-SIT-SITO- 221019/325
snowtide			07E1D107E 2017 10701		
pdfxstream					
Improper Input Validation	01-10-2019	4.3	In Snowtide PDFxStream before 3.7.1 (for Java), a crafted PDF file can trigger an extremely long running computation because of page- tree mishandling. CVE ID: CVE-2019-17063	N/A	A-SNO- PDFX- 221019/326
Sugarcrm					
sugarcrm					
CV Scoring Scal (CVSS)	e 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 Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by an Admin user. CVE ID: CVE-2019-17292	N/A	A-SUG- SUGA- 221019/327	
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Project module by a Regular user. CVE ID: CVE-2019-17293	N/A	A-SUG- SUGA- 221019/328	
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the export function by a Regular user. CVE ID: CVE-2019-17294	N/A	A-SUG- SUGA- 221019/329	
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the history function by a Regular user. CVE ID: CVE-2019-17295	N/A	A-SUG- SUGA- 221019/330	
Improper Neutralizatio n of Special Elements	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Contacts module by a Regular user.	N/A	A-SUG- SUGA- 221019/331	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			CVE ID : CVE-2019-17296		
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Quotes module by a Regular user. CVE ID: CVE-2019-17297	N/A	A-SUG- SUGA- 221019/332
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Administration module by a Developer user. CVE ID: CVE-2019-17298	N/A	A-SUG- SUGA- 221019/333
Improper Input Validation	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by an Admin user. CVE ID: CVE-2019-17299	N/A	A-SUG- SUGA- 221019/334
Improper Input Validation	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by a Developer user. CVE ID: CVE-2019-17300	N/A	A-SUG- SUGA- 221019/335
Improper Input Validation	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the ModuleBuilder module by an Admin user. CVE ID: CVE-2019-17301	N/A	A-SUG- SUGA- 221019/336

Weakness	Puk	blish Dat	e	CVSS	Description & CVE ID					Pa	tch	NCIIF	PC ID
Improper Input Validation	07-	10-201	9	6.5	before inject modu	CRM befe 9.0.2 allow ion in the left by a December 1. CVE-	IP code eBuilde r user.		I/A		A-SUG- SUGA- 22101		
						CRM bef			x				
Improper Input Validation	07-	10-201	9	6.5	inject	e 9.0.2 al ion in th lle by a D	e Merge	Records	S N	N/A		A-SUG- SUGA- 22101	
					CVE I	D : CVE-	2019-1	7303					,
Improper Input Validation	07-	10-201	9	6.5	before inject	CRM befe 9.0.2 alion in the	llows PH e Merge	IP code Records		I/A		A-SUG- SUGA- 22101	
					CVE I	D : CVE-	2019-1	7304					
Improper Input Validation	07-	10-201	9	6.5	before inject	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by a Regular user.					N/A		9/340
					CVE I	D : CVE-	2019-1	7305					
Improper Input Validation	07-	10-201	9	6.5	befor inject	CRM bef e 9.0.2 al ion in th lle by an	llows PH e Config	IP code urator		I/A		A-SUG- SUGA- 22101	
					CVE I	D : CVE-	2019-1	7306					
Improper Input Validation	07-	10-201	9	6.5	before inject	CRM befe 9.0.2 alion in the le by an	llows PH e Tracke	IP code er		I/A		A-SUG- SUGA- 22101	
					CVE I	D : CVE-	2019-1	7307					
Improper Input Validation	07-	10-201	9	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Emails module by a Regular user. CVE ID: CVE-2019-17308					N/A		A-SUG- SUGA- 22101	
Improper Input	07-	10-201	9	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code				X N	I/A		A-SUG-	-
CV Scoring Scal (CVSS)	e	0-1		1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

Weakness	Pu	blish Date	CVSS		Descript	ion & CV	E ID		Patch	NCIII	PC ID
Validation				modu	ion in th le by an D : CVE -	Admin	user.			22101	9/344
Improper Input Validation	07-	-10-2019	6.5	befor inject modu	CRM be e 9.0.2 a ion in that e by an D : CVE-	llows Ph le Campa Admin	HP code aigns user.	x N/A	Α	A-SUG SUGA- 22101	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-	-10-2019	6.5	befor trave funct	CRM be e 9.0.2 a rsal in th ion by a D : CVE -	llows di 1e attach Regular	rectory iment user.	x N/A	Α	A-SUG SUGA- 22101	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-	-10-2019	6.5	befor trave a Reg	CRM be e 9.0.2 a rsal in th ular use D : CVE -	llows di 1e file fu r.	rectory nction b		A	A-SUG SUGA- 22101	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-	-10-2019	6.5	befor trave by a I	CRM be e 9.0.2 a rsal in th Develope D : CVE -	llows di ne Studio er user.	rectory o module		A	A-SUG- SUGA- 221019/348	
Improper Limitation of a Pathname to a Restricted Directory ('Path	07-	-10-2019	6.5	befor trave modu	·CRM be e 9.0.2 a rsal in th lle by an D : CVE -	llows di ne Config Admin	rectory gurator user.	x N/A	Δ	A-SUG SUGA- 22101	
CV Scoring Scal (CVSS)	e	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
Traversal')					
Improper Input Validation	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Administration module by an Admin user. CVE ID: CVE-2019-17315	N/A	A-SUG- SUGA- 221019/350
Improper Input Validation	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Import module by a Regular user. CVE ID: CVE-2019-17316	N/A	A-SUG- SUGA- 221019/351
Improper Input Validation	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the UpgradeWizard module by an Admin user. CVE ID: CVE-2019-17317	N/A	A-SUG- SUGA- 221019/352
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by a Regular user. CVE ID: CVE-2019-17318	N/A	A-SUG- SUGA- 221019/353
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	07-10-2019	6.5	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Emails module by a Regular user. CVE ID: CVE-2019-17319	N/A	A-SUG- SUGA- 221019/354
Tcpdump					
tcpdump					

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	1.2	2 3	J 1	7	3 0	0 /	, 0	O J	3 10

Weakness	Pu	blish Date	cvss		Descript	ion & CV	E ID	Р	atch	NCIII	PC ID
Improper Input Validation	03-	-10-2019	7.5	in pri befor boun	orint_dat nt-lmp.c e 4.9.3 la ds check D : CVE -	in tcpdi icks cert s.	ump	hub. he- tcpd grou ump mit/ e0aa 234 458	s://git com/t ump- up/tcpd o/com 0b661 a61850 b6439 5cf577	A-TCP TCPD- 22101	
libpcap											
Improper Input Validation	03-	-10-2019	5	befor certain of reu open involved	od/daem e 1.9.1 m in length use of a v up an at ving extr equest. D : CVE -	nishandl values ariable. tack vec a data a	es because This ma tor t the end	hub. he- tcpd grou cap/ bpca 1.9/ GES http hub. he- tcpd grou cap/ t/61 033 91d 6190 495 http ww. mp.a	cHAN s://git com/t lump- ip/libp commi 7b12c 9db48 117b6 82126c 439ea, s://w tcpdu org/pu cve-	A-TCP 22101	
Insufficient Verification of Data	03-	-10-2019	5	befor	od/daem e 1.9.1 o orms pro	n non-W	/indows		s://git com/t	A-TCP-LIBP- 221019/357	
CV Scoring Sca (CVSS)	le	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
Authenticity			about why authentication failed, which might make it easier for attackers to enumerate valid usernames. CVE ID: CVE-2019-15162	tcpdump- group/libp cap/blob/li bpcap- 1.9/CHAN GES, https://git hub.com/t he- tcpdump- group/libp cap/commi t/484d60c bf7ca4ec75 8c3cbb8a8 2d68b244a 78d58, https://w ww.tcpdu mp.org/pu blic-cve- list.txt	
NULL Pointer Dereference	03-10-2019	5	rpcapd/daemon.c in libpcap before 1.9.1 allows attackers to cause a denial of service (NULL pointer dereference and daemon crash) if a crypt() call fails. CVE ID: CVE-2019-15163	https://git hub.com/t he- tcpdump- group/libp cap/blob/li bpcap- 1.9/CHAN GES, https://git hub.com/t he- tcpdump- group/libp cap/commi t/437b273 761adedcb d880f714b fa44afeec1	A-TCP-LIBP- 221019/358
CV Scoring Scal (CVSS)	e 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
				86a31, https://w ww.tcpdu mp.org/pu blic-cve- list.txt	
Server-Side Request Forgery (SSRF)	03-10-2019	5	rpcapd/daemon.c in libpcap before 1.9.1 allows SSRF because a URL may be provided as a capture source. CVE ID: CVE-2019-15164	https://git hub.com/t he- tcpdump- group/libp cap/blob/li bpcap- 1.9/CHAN GES, https://git hub.com/t he- tcpdump- group/libp cap/commi t/33834cb 2a4d035b5 2aa2a2674 2f832a112 e90a0a, https://w ww.tcpdu mp.org/pu blic-cve- list.txt	A-TCP-LIBP- 221019/359
Improper Input Validation	03-10-2019	5	sf-pcapng.c in libpcap before 1.9.1 does not properly validate the PHB header length before allocating memory. CVE ID: CVE-2019-15165	https://git hub.com/t he- tcpdump- group/libp cap/blob/li bpcap- 1.9/CHAN GES, https://git	A-TCP-LIBP- 221019/360
CV Scoring Scal (CVSS)	e 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	P	atch	NCIII	PC ID	
								com/t lump- lip/libp commi d6bef 062f96 0fa40c fd945d 0ab, s://w tcpdu org/pu cve- ext		
Teampass										
teampass										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	05-10-2019	3.5	Stored by set for an	Pass 2.1 d XSS at ting a cr item in D : CVE-	the Sear afted pa any fold	ch page Issword Ier.			A-TEA TEAM- 22101	-
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	05-10-2019	3.5	TeamPass 2.1.27.36 allows Stored XSS by setting a crafted Knowledge Base label and adding any available item. CVE ID: CVE-2019-17204						A-TEA TEAM- 22101	-
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	05-10-2019	4.3	Stored paylo durin an add	Pass 2.1 d XSS by ad in the g a login ministra	placing userna attemp tor look	a me field t. When s at the	111/73		A-TEA- TEAM- 221019/363	
CV Scoring Scal (CVSS)	e 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')			payload will be executed.		
			CVE ID : CVE-2019-17205		
themeisle					
visualizer					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	03-10-2019	4.3	A stored XSS vulnerability in the Visualizer plugin 3.3.0 for WordPress allows an unauthenticated attacker to execute arbitrary JavaScript when an admin or other privileged user edits the chart via the admin dashboard. This occurs because classes/Visualizer/Gutenberg/Block.php registers wp-json/visualizer/v1/update-chart with no access control, and classes/Visualizer/Render/Pa ge/Data.php lacks output sanitization. CVE ID: CVE-2019-16931	N/A	A-THE-VISU- 221019/364
Tibco					
master_data_	management				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	09-10-2019	3.5	The MDM server component of TIBCO Software Inc's TIBCO MDM contains multiple vulnerabilities that theoretically allow an authenticated user with specific roles to perform crosssite scripting (XSS) attacks. This issue affects TIBCO Software Inc.'s TIBCO MDM version 9.0.1 and prior versions; version 9.1.0. CVE ID: CVE-2019-11212	http://ww w.tibco.co m/services /support/a dvisories, https://w ww.tibco.c om/suppor t/advisorie s/2019/10 /tibco- security- advisory- october-8- 2019-	A-TIB-MAST- 221019/365
CV Scoring Scal (CVSS)	e 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
				tibco-mdm	
Twitter					
twitter_kit					
Improper Certificate Validation	07-10-2019	5.8	The Twitter Kit framework through 3.4.2 for iOS does not properly validate the api.twitter.com SSL certificate. Although the certificate chain must contain one of a set of pinned certificates, there are certain implementation errors such as a lack of hostname verification. NOTE: this is an end-of-life product. CVE ID: CVE-2019-16263	N/A	A-TWI- TWIT- 221019/366
Umbraco					
umbraco					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	02-10-2019	7.5	In Umbraco 7.3.8, there is SQL Injection in the backoffice/PageWApprove/PageWApproveApi/GetInpectSearch method via the nodeName parameter. CVE ID: CVE-2019-13957	N/A	A-UMB- UMBR- 221019/367
vanderbilt					
redcap					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	04-10-2019	3.5	REDCap before 9.3.4 has XSS on the Customize & Manage Locking/E-signatures page via Lock Record Custom Text values. CVE ID: CVE-2019-17121	N/A	A-VAN- REDC- 221019/368
Vbulletin					

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		Patch	NCIII	PC ID
vbulletin										
Files or Directories Accessible to External Parties	04-10-2019	6.4	misha within file ar direct	etin thro andles ex n the /co nd the /co cories. D : CVE-	cternal U ore/vb/v ore/vb/	N/A	1	A-VBU VBUL- 22101		
Improper Restriction of Rendered UI Layers or Frames	04-10-2019	4.3	clickja	etin befo acking. D : CVE-			N/A	Δ	A-VBU VBUL- 22101	
Improper Input Validation	04-10-2019	6.8	misha	etin thro andles cu D : CVE-	istom av	atars.	N/A	Λ	A-VBU VBUL- 22101	
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	08-10-2019	4	Inject ajax/a ajax/a t whe	etin 5.5.4 ion via t api/hool api/widg re paran D : CVE-	he x/getHo get/getV neter.	okList o VidgetLi	NI / /	1	A-VBU VBUL- 22101	
webarxsecuri	ity		•							
webarx										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	06-10-2019	4.3	The WebARX plugin 1.3.0 for WordPress has unauthenticated stored XSS via the URI or the X-Forwarded-For HTTP header. CVE ID: CVE-2019-17213					Δ	A-WEE WEBA 22101	-
Incorrect Authorizatio n	06-10-2019	5	Word	VebARX Press all ss by app	ows fire	o N/A	Λ	A-WEB- WEBA- 221019/374		
CV Scoring Scal (CVSS)	e 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	NCIIF	PC ID
			CVE I	D : CVE-	2019-1	7214				
webpagetest										
webpagetest										
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-10-2019	5	WebF Wind Trave arbitr unand expre by the	www/getfile.php in WPO VebPageTest 19.04 on Vindows allows Directory Traversal (for reading rbitrary files) because of an nanchored regular xpression, as demonstrated by the a.jpg\ substring. EVE ID: CVE-2019-17199					A-WEE WEBP- 22101	<u>-</u>
whatsapp										
whatsapp										
Double Free	03-10-2019	7.5	the Didecood libpl_ 1.2.15 for Ar allow execu	A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif before 1.2.15, as used in WhatsApp for Android before 2.19.244, allows remote attackers to execute arbitrary code or cause a denial of service. CVE ID: CVE-2019-11932				os://w .facebo com/sec y/advis es/cve- 9- 32	A-WHAT 22101	-
Wolfssl										
wolfssl										
Information Exposure Through Discrepancy	03-10-2019	1.2	wolfSSL and wolfCrypt 4.0.0 and earlier (when configured withoutenable-fpecc, enable-sp, orenable-sp-math) contain a timing side channel in ECDSA signature generation. This allows a local attacker, able to precisely measure the duration of signature operations, to infer information about the nonces used and potentially mount a				1	N/A		 9/377
CV Scoring Scal (CVSS)	e 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	atch	NCIII	PC ID
			privat occur multi bit lei	e attack to te key uses because plication of the transfer of transfer of the transfer of the transfer of the transfer of the transfer of trans	ed. The e ecc.c s might l	issue calar eak the				
			CVEI	D:CVE-	2019-1	3040				
wpfactory	uging and the	mag fr	iom da	shhoon						
download_plu	igins_and_the	mes_m	•				<u> </u>		Ι	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	07-10-2019	4.3	down settin plugin throu has m	des/setti load-plu gs.php in ns-dashb gh 1.5.0 nultiple u d XSS iss	gins- n the do oard plu for Wor inauther	wnload- ugin dPress	N/A		A-WPF DOWN 22101	-
Scripting')			CVE I	D : CVE-	2019-1	7239				
Xnview										
xnview										
Out-of- bounds Write	08-10-2019	4.6	User l at Xwsq	w Classi Mode Wi +0x0000 D : CVE -	rite AV s	tarting	N/A		A-XNV 22101	
Out-of- bounds Write	08-10-2019	4.6	User l at Xwsq	ew Classi Mode Wi +0x0000 D : CVE -	rite AV s	tarting	N/A		A-XNV 22101	-
xunruicms										
xunruicms										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	01-10-2019	3.5	An issue was discovered in XunRuiCMS 4.3.1. There is a stored XSS in the module_category area. CVE ID: CVE-2019-17074						A-XUN XUNR- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Puk	olish Dat	e CVSS		Descript	ion & CV	E ID		Pa	itch	NCIII	PC ID
Scripting')												
zingbox												
inspector												
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	09-	10-201	9 9	vulne Zingh 1.286 for ar execu	A command injection vulnerability exists in the Zingbox Inspector versions 1.286 and earlier, that allows for an authenticated user to execute arbitrary system commands in the CLI. CVE ID: CVE-2019-15014 An SOL injection vulnerability						A-ZIN- 22101	_
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	09-	10-201	9 6.5	exists interference that a data passe the d	An SQL injection vulnerability exists in the management interface of Zingbox Inspector versions 1.288 and earlier, that allows for unsanitized data provided by an authenticated user to be passed from the web UI into the database. CVE ID: CVE-2019-15016						A-ZIN- 22101	
Improper Authenticati on	09-	10-201	9 5	in the version wher requi Inspe- differ	A security vulnerability exists in the Zingbox Inspector versions 1.280 and earlier, where authentication is not required when binding the Inspector instance to a different customer tenant. CVE ID: CVE-2019-15018				/A		A-ZIN- 22101	
Improper Input Validation	09-	10-201 ⁽	9 7.5	in the version that of supplications updated and the left of the l	A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector. CVE ID: CVE-2019-15019				/A		A-ZIN- 22101	
CV Scoring Scal (CVSS)	e	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 Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	09-10-2019	7.5	A security vulnerability exists in the Zingbox Inspector versions 1.293 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector that could result in command injection. CVE ID: CVE-2019-15020	N/A	A-ZIN-INSP- 221019/386
Information Exposure	09-10-2019	5	A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that can allow an attacker to easily identify instances of Zingbox Inspectors in a local area network. CVE ID: CVE-2019-15021	N/A	A-ZIN-INSP- 221019/387
Authenticati on Bypass by Spoofing	09-10-2019	5	A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that allows for the Inspector to be susceptible to ARP spoofing. CVE ID: CVE-2019-15022	N/A	A-ZIN-INSP- 221019/388
Cleartext Storage of Sensitive Information	09-10-2019	5	A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that results in passwords for 3rd party integrations being stored in cleartext in device configuration. CVE ID: CVE-2019-15023	N/A	A-ZIN-INSP- 221019/389
Improper Input Validation	09-10-2019	6.8	A security vulnerability exists in Zingbox Inspector version 1.293 and earlier, that allows for remote code execution if the Inspector were sent a malicious command from the Zingbox cloud, or if the Zingbox Inspector were	N/A	A-ZIN-INSP- 221019/390
CV Scoring Scal (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Description & CVE ID	Patch	NCIIPC ID
			tampered with to connect to		
			an attacker's cloud endpoint.		
			CVE ID: CVE-2019-1584		
Zohocorp					
manageengine	e_datasecurit	y_plus			
Files or Directories Accessible to External Parties	09-10-2019	4	An issue was discovered in Zoho ManageEngine DataSecurity Plus before 5.0.1 5012. An exposed service allows a basic user ("Operator" access level) to access the configuration file of the mail server (except for the password).	N/A	A-ZOH- MANA- 221019/391
			CVE ID: CVE-2019-17112		
			Operating System		
Canonical					
ubuntu_linux					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-10-2019	5	Unbound before 1.9.4 accesses uninitialized memory, which allows remote attackers to trigger a crash via a crafted NOTIFY query. The source IP address of the query must match an access-control rule. CVE ID: CVE-2019-16866	N/A	O-CAN- UBUN- 221019/392
Out-of- bounds Read	06-10-2019	7.5	libsoup from versions 2.65.1 until 2.68.1 have a heap-based buffer over-read because soup_ntlm_parse_challenge() in soup-auth-ntlm.c does not properly check an NTLM message's length before proceeding with a memcpy. CVE ID: CVE-2019-17266	N/A	O-CAN- UBUN- 221019/393
Checkpoint					

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	1-2	2-3	5	7	3-0	0-7	7-8	0-3	9-10

Weakness	Pu	blish Date	cvss		Descript	ion & CV	E ID	1	Patch	NCIII	PC ID		
gaia													
Improper Handling of Exceptional Conditions	02-	-10-2019	5	R80.3 before by Ch Mana unique	are scenarion of Securion of S	ty Gatev ke 50 m it R80.30 crashes uration ging.	way anaged 0 with a of	t N/A	1	O-CHE 22101	-GAIA- 9/394		
				CVE I	CVE ID : CVE-2019-8462								
Cisco		~											
firepower_93	00_f	irmwar	e							1			
Improper Encoding or Escaping of Output	02-	-10-2019	7.2	multi- Firepo (FTD) auther escap FTD ir comm privil name vulne insuff under attack vulne critica filesys could execu privil name the at	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.			e N/A	1	0-CIS- 22101	FIRE- 9/395		
Improper Encoding or Escaping of Output	02-	Firepower Threat Defense		multi-instance feature of Cisco				7.2 multi-instance feature of Cisco Firepower Threat Defense		O N/A	1	O-CIS-FIRE- 221019/396	
CV Scoring Scal (CVSS)	le	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
			authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675		
Improper Input Validation	02-10-2019	7.2	Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges. CVE ID: CVE-2019-12699	N/A	O-CIS-FIRE- 221019/397

(CVSS)

Weakness	Publish Date	cvss	Descrip	otion & CV	E ID	Р	atch	NCIII	PC ID
Uncontrolled Resource Consumption	02-10-2019	6.8	A vulnerability configuration Authentication used in Ciscon Threat Defends of tware, Ciscon Management Software, and Software conduthenticate to cause a defend (DoS) condition vulnerability improper resummanagement user session attacker country vulnerability an affected successful extends and the attacker resources and to reload, rescondition. To vulnerability needs valid to the system. CVE ID: CVI	on Modulo Firepowerse (FTD) sco Firepowerse (FTD) sco Firepowerse (FTD) sco Firepowerse (FTD) sco Firepowerse (FTD) scource (FTD	r N/A		0-CIS- 22101	FIRE- 9/398	
firepower_41	15_firmware								
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vultiple vultiple vultiple multi-instant Firepower T (FTD) Softwalthenticate escape the commands version with the	n N/A		0-CIS- 22101	FIRE- 9/399		
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

			privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host		
			namespace. This could allow the attacker to impact other running FTD instances.		
			CVE ID : CVE-2019-12674		
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675	N/A	O-CIS-FIRE- 221019/400
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	
firepower_41	25_firmware		L			
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.	N/A	O-CIS-FIRE- 221019/401	
			CVE ID : CVE-2019-12674			
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying	N/A	O-CIS-FIRE- 221019/402	

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Pub	lish Date	cvss	·					Patch	NCIII	PCID
				filesys could execu privil- name the at runni	al files or stem. A s allow th te comm eges wit space. T tacker to ng FTD i	successform attack ands whin the label in th	ul explo ter to ith root nost d allow t other s.	·			
firepower_414	45 fi	rmwar	e	CVET	D.CVE-	2019-1					
Improper Encoding or Escaping of Output	02-1	10-2019	7.2	multi- Firepo (FTD) authe escap FTD is comm privile name vulne insuff under attack vulne critica filesys could execu privile name the at runni	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12674				A	0-CIS- 22101	
Improper Encoding or Escaping of Output	02-1	10-2019	7.2	multi- Firepo (FTD) authe	ple vulno instance ower Th Softwan nticated e the con	e feature reat Def re could , local at	e of Cisco ense allow a ttacker t	0 N/A	Α	0-CIS- 22101	
CV Scoring Scale (CVSS)	e	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
			FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675		
firepower_41	10_firmware				
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow	N/A	O-CIS-FIRE- 221019/405

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		Patch	NCIII	PC ID
			runni	tacker to ng FTD i D : CVE-	nstance	S.				
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multipmulti- Firepo (FTD) auther escap FTD in common privile name will author insuff under attack vulne critical filesystems could execur privile name the attrunni	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675					0-CIS- 22101	
firepower_41	20_firmware									
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the				n o N/	/A	0-CIS- 22101	
CV Scoring Scal	le 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	
			underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12674								
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675				o n n n n n n n n n n n n n n n n n n n	/A		0-CIS- 22101	
firepower_4140_firmware											
Improper Encoding or Escaping of	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense					/A		0-CIS-FIRE- 221019/409	
CV Scoring Scal (CVSS)	e 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	NCIII	PC ID
Output			authe escap FTD is comm privile name vulne insuff under attack vulne critica filesys could execu privile name the at runni	Software nticated e the cornstance ands wing eges in the space. The rabilities of the could rabilities al files or stem. As allow the commerces with the commerces wi	the host hese sare due to tection esystem lexploit sby moderate attack ands within the lexploit of the impact and the lexploit of the uncompact and the lexploit of the lexplo					
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host					A	0-CIS- 22101	
CV Scoring Scal (CVSS)	e 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	NCII	PC ID
			namespace. This could allow the attacker to impact other running FTD instances.							
			CVE I	D : CVE-	2019-1	2675				
firepower_41	50_firmware									
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12674				n o N/A	A	0-CIS- 22101	
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to			o 1 0 1 1 1 1 1 1 1 1	A	0-CIS- 22101	FIRE- 9/412	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss		Descript	ion & CV	E ID		Patch	NCII	PC ID
				under attack vulne critica filesy, could execu privil name the at runni	icient procession of the country of the comme country of the count	esystem I exploit Is by mod In the un Is uccessfue attack In ands wi I his could I impact I instance	An these difying derlying ul exploser to ith root nost dallow to other s.	7			
fxos											
Improper Input Validation	02-	-10-2019	7.2	CLI of and C Defendation allow attack on the system privil vulne insuff An att vulne crafted explodattack on the on the control of the control on the contro	. cc					0-CIS- 22101	FXOS- 9/413
Uncontrolled Resource Consumption	02-	-10-2019	6.8	config Author used in Threa	Inerability in the iguration of the Pluggable entication Module (PAM) in Cisco Firepower eat Defense (FTD) ware, Cisco Firepower			A	0-CIS- 22101	FXOS- 9/414	
CV Scoring Scale (CVSS)	e	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
			Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system. CVE ID: CVE-2019-12700		
email_securit	y_appliance_f	irmwa	re		
Improper Input Validation	02-10-2019	5	A vulnerability in the Sender Policy Framework (SPF) functionality of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the configured user filters on an affected device. The vulnerability exists because the affected software insufficiently validates certain incoming SPF messages. An attacker could exploit this	N/A	O-CIS-EMAI- 221019/415

Weakness	Publish Date	CVSS		Descript	ion & CVI	E ID	Р	atch	NCIII	PC ID
			vulnerability by sending a custom SPF packet to an affected device. A successful exploit could allow the attacker to bypass the configured header filters, which could allow malicious content to pass through the device. CVE ID: CVE-2019-12706							
ic3000_indus	trial_compute	e_gatev	vay_fir	mware						
Uncontrolled Resource Consumption	02-10-2019	4	based of Cis Comp an au attack service affect vulne the affingred exploopenis simul web-kinterf A succallow DoS cobased prevention and attack service allow and attack service affect vulne the affingred exploopenis simul web-kinterf A succallow and attack service affects of the service affects of t	nerability manage co IC300 oute Gate thenticat ce (DoS) ed devic rability of fected so operly m rces. An it this vu ng a larg taneous based ma face of an cessful e the atta ondition manage onting no gement of	ement in 10 Indus way coursed, remuse a descendition. The exists been stacked anages sattacked anagement in affected condition of the verment in rmal operation.	terface trial ald allow ote nial of on on an ecause system c could ity by er of s on the ent d device ould cause a web- terface, ons.	N/A			
asa_5505_firn	nware									
Uncontrolled Resource Consumption	02-10-2019	7.8	Key E	nerabilit xchange 1) featui	version	1	N/A	N/A 0-CIS-A 221019		
CV Scoring Scal	e 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
			(ASA) Firepo (FTD) unaut attack an aff a dent condi due to of sys could by ser traffic The a valid authe nor de addre stater applie of the explo attack memo a relo	tive Seculoser The Software Chentical Software to trive teeted decial of sertion. The Dimproproproproproproproproproproproproprop	arity Appre and Careat Defere could ted, remarking are vice, reservice (Doe vulner per manalicious and this vulnation and the VPN attacker to matcacker to matcacker allow the haust syurces, leaffected affected affected affected affected affected and the very per and the crypteres and the crypteres and the very per and the very	coliance isco fense allow an ote eload of sulting in oS) ability is agement attacket erability IKEv1 levice. aneed session, s source h a peer to map interface An e extem ading to I device.				
asa_5510_firn	nware									
Uncontrolled Resource Consumption	02-10-2019	7.8	Key E (IKEv Adapt (ASA) Firepo (FTD) unaut attack an aff a den	xchange 1) featur tive Secur Softwar ower Th Softwar chenticat secr to tri ected de	e version re of Cis arity App re and Careat Def re could ted, rem agger a revice, res	co oliance isco Tense allow an ote eload of sulting in			0-CIS- 22101	-ASA -9/418
CV Scoring Scale	e 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
			due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256		
asa_5512-x_fi	rmware				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source	N/A	0-CIS-ASA 221019/419

1-2

0-1

CV Scoring Scale

(CVSS)

3-4

4-5

6-7

7-8

8-9

5-6

Weakness	Publish Date	cvss		Descript	ion & CV	E ID	P	atch	NCIII	PC ID
			stater applie of the explo attack memo	ess need ment in the ded to the affected it could after to expery resonad of an D: CVE-	the crypt ingress I device. allow th haust sy urces, le affected	to map interfact An e stem ading to				
asa_5515-x_fi	rmware									
Uncontrolled Resource Consumption	02-10-2019	7.8	Key E (IKEV Adapt (ASA) Firepo (FTD) unaut attack an aff a dent condi due to of sys could by sen traffic The a valid authe nor de addre stater applie of the explo attack memo a relo	nerability xchange 1) feature 1) feature 1 feature 2 fea	version re of Cis- re of Cis- re and Ci reat Def re could ted, rem gger a re vice, res vice (Do e vulners ber mana mory. Ar this vulr alicious fected d does not als to he VPN attacker' to match ingress I device. allow th haust sy urces, le affected	obliance isco ense allow arote eload of sulting in oS) ability is agement attacked erability. IKEv1 evice. need session, a peer to map interfact An e estem ading to device.	n n s s s s r y N/A		0-CIS- 22101	
CV Scoring Scal (CVSS)	e 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		Pat	ch	NCIII	PC ID
asa_5520_firm	nware	<u> </u>	'							<u>'</u>	
Uncontrolled Resource Consumption	02-10-2019	7.8	Key E (IKEV Adapt (ASA) Firepo (FTD) unaut attack an aff a dent condi due to of sys could by ser traffic The a valid authe nor de addre stater applie of the explo attack memo a relo	nerability xchange 1) feature ive Security Software The Software The Software in the ceted definition. The software in the ceted in the	version re of Cis re of Cis re of Cis re and C reat Def re could ded, rem gger a re vice, res vice (Do e vulner der man this vulr alicious fected d does not als to he VPN attacker' to match ingress I device. allow th haust sy urces, le affected	obliance isco lisco lisco lisco lense allow are obliance sulting in oS) ability is agement attacket herabilit levice. hered session, s source ha peer to map interface An e estem ading to I device.	n s t er N	/A		0-CIS- 22101	-
asa_5525-x_fi	rmware										
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote				N	/A		0-CIS- 22101	-
CV Scoring Scal (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
			attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256		
asa_5540_firm	nware				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device.	N/A	0-CIS-ASA 221019/423

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
			The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256		
asa_5545-x_fi	rmware				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the	N/A	O-CIS-ASA 221019/424

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			
			attacker to exhaust system memory resources, leading to a reload of an affected device.					
			CVE ID : CVE-2019-15256					
asa_5550_firm	iware							
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256	N/A	O-CIS-ASA 221019/425			
asa_5555-x_fii	rmware							
Uncontrolled Resource Consumption	02-10-2019	7.8	attacker to exhaust system memory resources, leading to a reload of an affected device.					
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		Descript	ion & CV	E ID	P	atch	NCII	PC ID
			(ASA) Firepo (FTD) unaut attack an aff a dent condi due to of sys could by ser traffic The a valid authe nor de addre stater applie of the explo attack memo a relo	tive Seculower The Software Chentical Act of Serition. The Dimpropression of the Exploit and an adding make to an adding make to an adding the Company of the Exploit and the	arity Appre and Careat Defere could ted, remarking are vice, reservice (Doe vulner per manalicious and this vulnation and the VPN attacker to matcacker to matcacker allow the haust syurces, leaffected affected affected affected affected and the crypere a	coliance isco fense allow an ote eload of sulting in oS) ability is agement attacker herability levice. aneed session, s source h a peer to map interface An e estem ading to I device.				
asa_5580_firn	nware									
Uncontrolled Resource Consumption	02-10-2019	7.8	Key E (IKEv Adapt (ASA) Firepo (FTD) unaut attack an aff a den	xchange 1) featur tive Secur Softwar ower Th Softwar chenticat ser to tri ected de	e version re of Cis arity App re and Careat Def re could ted, rem agger a revice, res	co oliance isco Tense allow an ote eload of sulting in			0-CIS- 22101	-ASA -9/427
CV Scoring Scale	e 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		Descript	ion & CV	E ID		Patch	NCIII	C ID
			of sys could by ser traffic The a valid authe nor do addre stater applie of the explo- attack memo a relo	tem men exploit ding ma to an af ttacker of credenti nticate to es the a ss need nent in the affected it could a ter to ex	mory. And this vulnations of the deciral to the crypton of the cry	session, s source h a peer to map interface An e extern ading to I device.	er y			
compal										
ch7465lg_firm	nware									
Improper Input Validation	02-10-2019	7.5	NCIP- device Contr Input can se modif conta which device endpe	6.12.18. es have lol becau Validatiend a ma ied POS ining show will be	24-5p8- Incorrect Incorrec	et Access proper attacker y of request nands, d on the API modem.	st N/	A	O-COM CH74- 22101	
Debian										
debian_linux										
Improper Input Validation	01-10-2019	7.5	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either							
CV Scoring Scal (CVSS)	le 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
			globally or for a specific property) for an externally exposed JSON endpoint and the service has the commonsdbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of org.apache.commons.dbcp.dat asources.SharedPoolDataSour ce and org.apache.commons.dbcp.dat asources.PerUserPoolDataSour ce mishandling.		
Improper Input Validation	01-10-2019	7.5	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy.P6DataS ource mishandling.	N/A	O-DEB-DEBI- 221019/430
fiberhome					
hg2201t_firm		_			
Improper	08-10-2019	5	/var/WEB-GUI/cgi-	N/A	O-FIB-HG22-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 157	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID	1	Patch	NCIIF	PC ID	
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			bin/downloadfile.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows pre- authentication Directory Traversal for reading arbitrary files. CVE ID: CVE-2019-17187						22101	9/431	
FON											
fon2601e-se_	fon2601e-se_firmware										
Improper Input Validation	04-10-2019	7.8	FON2 FON2 firmw earlie they r resolv is exp be lev ampli other	601E-SE 601E-FS 601E-FS vare vers r contain may beha vers. If the loited, F veraged f fication entities. D: CVE-	SW-S, and SW-B with sions 1.1 an issurance as of the side of the s	d th .7 and le where pen erability ers may	e N/A	1	0-F0N F0N2- 22101		
fon2601e-re_	firmware										
Improper Input Validation	04-10-2019	7.8	FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities. CVE ID: CVE-2019-6015			e N/A	Α	0-F0N F0N2- 22101			
fon2601e-fsw	y-s_firmware										
Improper Input	04-10-2019	7.8		601E-SE 601E-FS			., N/A	A	O-FON FON2-	-	
CV Scoring Scal (CVSS)	e 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		Patch	NCIIF	PC ID
Validation			earlie they r resolv is exp be lev ampli other	firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities. CVE ID: CVE-2019-6015					22101	9/434
fon2601e-fsw	y-b_firmware						I		ı	
Improper Input Validation	04-10-2019	7.8	FON2 FON2 firmw earlie they r resolv is exp be lev ampli other	601E-SE 601E-FS vare vers r contain may behavers. If the loited, Foreraged for the fication entities. D: CVE-	SW-S, an SW-B wisions 1.1 an issuave as opinis vulne for DNS attacks	d th7 and ie where pen erability ers may	e N/	A	0-F0N F0N2- 22101	
Google							l e		ı	
chrome_os										
Integer Overflow or Wraparound	01-10-2019	9.3	The Imagination Technologies driver for Chrome OS before R74-11895.B, R75 before R75-12105.B, and R76 before R76-12208.0.0 allows attackers to trigger an Integer Overflow and gain privileges via a malicious application. This occurs because of intentional access for the GPU process to /dev/dri/card1 and the PowerVR ioctl handler, as demonstrated by PVRSRVBridgeSyncPrimOpCre				5- - N/	A	0-G00 CHRO- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID	
			ate. CVE I	D : CVE-	2019-1	6508					
govicture											
pc530_firmwa	are										
Missing Authenticati on for Critical Function	01-10-2019	10	unaut acces	re PC53(chenticat s as root D : CVE-	ed TELN	NET	N/A	1	0-G0V PC53- 22101		
Linux											
linux_kernel	inux_kernel										
Incorrect Default Permissions	01-10-2019	2.1	net/a AF_AZ the Li does i CAP_I that u create 0614	create in x25/af_a x25 network content of the conte	ax25.c in vork mo nel throu rce W, which ged usen ocket, al 88. 2019-1	dule in 1gh 5.3.2 1 means 1's can 1's can	NI / A	1	0-LIN- 22101		
Incorrect Default Permissions	01-10-2019	2.1	net/ic the Al modu throu CAP_I that u create e69dl	02154_c eee8021 F_IEEE80 lle in the gh 5.3.2 NET_RAV inprivile e a raw s od4619e D : CVE -	54/sock 02154 n Linux k does no W, which ged user ocket, al 7.	etwork ernel t enforc n means rs can ka CID-	NI / /	1	0-LIN- 22101		
Incorrect Default Permissions	01-10-2019	2.1	atalk_create in net/appletalk/ddp.c in the AF_APPLETALK network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can					1	0-LIN- 22101		
CV Scoring Scal (CVSS)	e 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			E ID	F	atch	NCIIF	PC ID
			6cc03	e a raw s Be8aa36	C					
				CVE ID : CVE-2019-17054						
Improper Input Validation	01-10-2019	2.1	driver in the modu throu CAP_I that u create b91ee	sock_cre rs/isdn/ rs/isdn/ AF_ISDI le in the gh 5.3.2 NET_RAV inprivile e a raw s e4aa2a2 D: CVE-	mISDN/ N netwo Linux k does no W, which ged user ocket, al	rk ernel t enforce n means rs can ka CID-	e N / A		0-LIN- 22101	
Incorrect Default Permissions	01-10-2019	2.1	net/n AF_NI Linux does I CAP_I that u create	ock_creatic/llcp_s FC network kernel to the enformation NET_RAN Imprivile a raw s 9798b17 D: CVE-	ock.c in ork mod hrough rce W, which ged user ocket, al	ule in th 5.3.2 n means rs can ka CID-	e N/A		0-LIN- 22101	
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-10-2019	7.1	An issue was discovered in write_tpt_entry in drivers/infiniband/hw/cxgb4 /mem.c in the Linux kernel through 5.3.2. The cxgb4 driver is directly calling dma_map_single (a DMA function) from a stack variable. This could allow an attacker to trigger a Denial of Service, exploitable if this driver is used on an architecture for which this stack/DMA interaction has security relevance. CVE ID: CVE-2019-17075				N/A		0-LIN- 22101	
CV Scoring Scal	e 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		Descript	ion & CV	E ID	F	atch	NCIIF	PC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-10-2019	7.5	In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow. CVE ID: CVE-2019-17133						0-LIN- 22101	
Uncontrolled Resource Consumption	08-10-2019	4.9	drive Linux used i allow cause becau resou the m	An issue was discovered in drivers/xen/balloon.c in the Linux kernel before 5.2.3, as used in Xen through 4.12.x, allowing guest OS users to cause a denial of service because of unrestricted resource consumption during the mapping of guest memory, aka CID-6ef36ab967c7.					0-LIN- 22101	
Microsoft										
windows										
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	07-10-2019	7.5	befor attack comm methor for co	eX Contre 6.2.203 ker to exemand via od. This de execu	19.814 a ecute ar the Shel can be le	llow an bitrary llOpen everaged	N/A		0-MIC- WIND- 22101	
Improper Input Validation	07-10-2019	7.5	MyBuilder viewer before 6.2.2019.814 allow an attacker to execute arbitrary command via specifically crafted configuration file. This can be leveraged for code execution. CVE ID: CVE-2019-12812			6.2.2019.814 allow an attacker to execute arbitrary command via specifically crafted configuration file. This can be leveraged for code execution.			O-MIC- WIND- 22101	
Use After Free	04-10-2019	6.8	This vulnerability allows remote atackers to execute				N/A		O-MIC- WIND-	
CV Scoring Scal	e 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		Patch	NCIII	PC ID
			arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.						22101	9/448
Use After Free	04-10-2019	6.8	remo arbitr instal Phant User i explo that t malic exists Calcu result valida object opera attack vulne in the proce	This vulnerability allows remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8757.				/A	O-MIC- WIND- 22101	9/449
Use After	04-10-2019	6.8	This vulnerability allows			N,	'A	O-MIC	-	
CV Scoring Scal (CVSS)	e 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	ID	F	atch	NCIII	PC ID
Free			remote atackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759. CVE ID: CVE-2019-13317						WIND- 22101	
Use of Externally- Controlled Format String	04-10-2019	4.3	This verse in terms of sensite affect Reade interaction in the sexual control of the sex	vulnerabete attack rive informed instaler 9.5.0.2 action is it this vulne target ious file. within the tall.printfod. The assess the rmat straddresse script. Ange this in the code in trent printformat straddresse script. Ange this in the code in trent printformat straddresse script. Ange this in the code in trent printformat straddresse script. Ange this in the code in trent printformat straddresse script.	ility allo ers to di mation lations of 20723. U required linerabil t must v e or ope The spec Javascri pplicati %p para ing, allo es to be in linerabili in the co	ws sclose on of Foxit ser d to ity in isit a n a cific flav essing of pt on ameter in wing returned xer can nction ties to ntext of	n N/A		O-MIC- WIND- 22101	
CV Scoring Scal (CVSS)	e 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
			CAN-8544. CVE ID : CVE-2019-13318		
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.	N/A	O-MIC- WIND- 221019/452
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current	N/A	O-MIC- WIND- 221019/453
CV Scoring Scal (CVSS)	le 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
			process. Was ZDI-CAN-8814. CVE ID: CVE-2019-13320		
Out-of- bounds Write	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8783.	N/A	O-MIC- WIND- 221019/454
Out-of- bounds Read	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIFF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated	N/A	O-MIC- WIND- 221019/455
CV Scoring Scal (CVSS)	e 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
			structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8782.		
			CVE ID : CVE-2019-13324		
Out-of- bounds Read	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8922.	N/A	O-MIC- WIND- 221019/456
			CVE ID : CVE-2019-13325		
Out-of- bounds Read	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue	N/A	O-MIC- WIND- 221019/457
CV Scoring Scal (CVSS)	e 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	Pat	tch	NCIIPC ID
			results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8864. CVE ID: CVE-2019-13326			
Use After Free	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8888.	N/A		O-MIC- WIND- 221019/458
Use After Free	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the	N/A		O-MIC- WIND- 221019/459
CV Scoring Scal (CVSS)	e 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
Access of Resource Using Incompatible	03-10-2019	6.8	processing of fields within Acroform objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8913. CVE ID: CVE-2019-13328 This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIF files. The	N/A	O-MIC- WIND-
Type ('Type Confusion')			issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8695. CVE ID: CVE-2019-13329		221019/460
Access of Resource Using Incompatible Type ('Type Confusion')	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The	N/A	O-MIC- WIND- 221019/461
CV Scoring Scal	e 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
			specific flaw exists within the processing of JPG files. The issue results from the lack of proper validation of usersupplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8742.		
Out-of- bounds Read	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8838.	N/A	O-MIC- WIND- 221019/462
Use After Free	03-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or	N/A	O-MIC- WIND- 221019/463
CV Scoring Scale (CVSS)	e 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	Р	atch	NCIII	PC ID
			specific process forms the lace existe perform object leveral execution the current can be considered as a constant of	open a malicious file. The specific flaw exists within the processing of templates in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9149. CVE ID: CVE-2019-13332						
Allocation of Resources Without Limits or Throttling	01-10-2019	7.5	PuTTY before 0.73 on Windows improperly opens port-forwarding listening sockets, which allows attackers to listen on the same port to steal an incoming connection. CVE ID: CVE-2019-17067				N/A		O-MIC- WIND- 22101	
Missing Release of Resource after Effective Lifetime	04-10-2019	5	an Acc if insu		ation ar memory				O-MIC- WIND- 22101	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-10-2019	5	www/getfile.php in WPO WebPageTest 19.04 on Windows allows Directory Traversal (for reading arbitrary files) because of an unanchored regular expression, as demonstrated by the a.jpg\ substring. CVE ID: CVE-2019-17199			N/A		O-MIC- WIND- 22101		
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected				N/A		0-MIC- WIND- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
			installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deleteItemAt method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295.							
Use After Free	04-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.				N/A		O-MIC- WIND- 22101	9/468
Use After	04-10-2019	6.8	This vulnerability allows				N/A	Λ	O-MIC-	-
CV Scoring Scale (CVSS)	e 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		Pat	ch	NCIII	PC ID		
Free			remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing watermarks within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8801.							WIND- 22101			
Authenticati on Bypass by Spoofing	10-10-2019	4.3	when not processed conte Brow Vulne uniqu	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.				when Microsoft Browsers does ot properly parse HTTP ontent, aka 'Microsoft rowser Spoofing 'ulnerability'. This CVE ID is				O-MIC WIND- 22101	-
Improper Restriction of XML External Entity Reference ('XXE')	10-10-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1060					'A		O-MIC WIND- 22101	-		
CV Scoring Scal (CVSS)	e 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 Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE- 2019-1239. CVE ID: CVE-2019-1238	N/A	O-MIC- WIND- 221019/472
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE- 2019-1238. CVE ID: CVE-2019-1239	N/A	O-MIC- WIND- 221019/473
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019- 1366. CVE ID: CVE-2019-1307	N/A	O-MIC- WIND- 221019/474
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307,	N/A	O-MIC- WIND- 221019/475

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1335, CVE-2019- 1366. CVE ID : CVE-2019-1308		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1311	N/A	O-MIC- WIND- 221019/476
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.	N/A	O-MIC- WIND- 221019/477
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1316	N/A	O-MIC- WIND- 221019/478
Improper Link Resolution Before File Access ('Link Following')	10-10-2019	5.6	A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'. CVE ID: CVE-2019-1317	N/A	O-MIC- WIND- 221019/479
CV Scoring Scal (CVSS)	e 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
Information Exposure	10-10-2019	4.3	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.	N/A	O-MIC- WIND- 221019/480
Improper Privilege Management	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1319		O-MIC- WIND- 221019/481		
Improper Authenticati on	10-10-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340. CVE ID: CVE-2019-1320	N/A	O-MIC- WIND- 221019/482
Improper Authenticati on	10-10-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340. CVE ID: CVE-2019-1322	N/A	O-MIC- WIND- 221019/483
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not	N/A	O-MIC- WIND- 221019/484
CV Scoring Scale (CVSS)	e 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
			properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336. CVE ID: CVE-2019-1323		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	4.9	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1325	N/A	O-MIC- WIND- 221019/485
Improper Input Validation	10-10-2019	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. CVE ID: CVE-2019-1326	N/A	O-MIC- WIND- 221019/486
Improper Input Validation	10-10-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1333	N/A	O-MIC- WIND- 221019/487

Weakness	Publish Date	cvss		Descript	ion & CVI	E ID		Patch	NCIII	PC ID				
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	that the engine memore control of the control of th	nerability exists in the way t the Chakra scripting gine handles objects in mory in Microsoft Edge, aka akra Scripting Engine mory Corruption nerability'. This CVE ID is que from CVE-2019-1307, E-2019-1308, CVE-2019-			a N/A	A	O-MIC- WIND- 22101					
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.					vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is				Λ	O-MIC- WIND- 22101	
Information Exposure	10-10-2019	2.1	vulne Wind handl aka 'V Inforr Vulne uniqu	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1334. CVE ID: CVE-2019-1345					O-MIC- WIND- 22101					
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357				when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.							
CV Scoring Scal (CVSS)	e 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 Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019 7.6		vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307,		that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.		O-MIC- WIND- 221019/492
. 1			CVE ID : CVE-2019-1366				
windows_7							
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357. CVE ID: CVE-2019-0608	N/A	O-MIC- WIND- 221019/493		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239. CVE ID: CVE-2019-1238	N/A	O-MIC- WIND- 221019/494		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1311	N/A	O-MIC- WIND- 221019/495		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342. CVE ID: CVE-2019-1315	N/A	O-MIC- WIND- 221019/496
Information Exposure	10-10-2019	4.3	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'. CVE ID: CVE-2019-1318	N/A	O-MIC- WIND- 221019/497
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1319	N/A	O-MIC- WIND- 221019/498
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	4.9	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.	N/A	O-MIC- WIND- 221019/499
CV Scoring Scal (CVSS)	e 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
			CVE ID : CVE-2019-1325		
Improper Input Validation	10-10-2019	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. CVE ID: CVE-2019-1326	N/A	O-MIC- WIND- 221019/500
Improper Input Validation	10-10-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1333	N/A	O-MIC- WIND- 221019/501
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357	N/A	O-MIC- WIND- 221019/502
Information Exposure	10-10-2019	4.3	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'. CVE ID: CVE-2019-1361	N/A	O-MIC- WIND- 221019/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	10-10-2019	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. CVE ID: CVE-2019-1363	N/A	O-MIC- WIND- 221019/504
windows_8.1					
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357. CVE ID: CVE-2019-0608	N/A	O-MIC- WIND- 221019/505
Improper Restriction of XML External Entity Reference ('XXE')	10-10-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1060	N/A	O-MIC- WIND- 221019/506
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239. CVE ID: CVE-2019-1238	N/A	O-MIC- WIND- 221019/507
Improper Restriction	10-10-2019	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC- WIND-

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1311		221019/508
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342. CVE ID: CVE-2019-1315	N/A	O-MIC- WIND- 221019/509
Information Exposure	10-10-2019	4.3	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'. CVE ID: CVE-2019-1318	N/A	O-MIC- WIND- 221019/510
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1319	N/A	O-MIC- WIND- 221019/511
Improper Restriction of Operations within the	10-10-2019	4.9	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system	N/A	O-MIC- WIND- 221019/512
CV Scoring Scal (CVSS)	e 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	Р	atch	NCII	PC ID
Bounds of a Memory Buffer			local for 32 'Wind Buffe Privil	operly hacalls wit 2-bit systlows Red ring Systlege Vulr D: CVE-	hin Win tems, ak directed tem Elev terabilit	dows 7 a Drive vation of y'.				
Improper Input Validation	10-10-2019	7.8	vulne Deskt an att targe sends reque Remo (RDP) Vulne	•	exists in ocol (RD onnects using R y crafte 'Window top Prot of Servi	DP and d ws ocol ce			O-MIC WIND- 22101	-
Improper Input Validation	10-10-2019	9.3	A rem vulne Wind Client a mal 'Remo Remo Vulne	note code rability ows Ren t when a icious se ote Desk ote Code erability'	e execut exists in note Des user co erver, ak top Clie Executi	ion the sktop nnects to a nt on	N/A		O-MIC WIND- 22101	
Authenticati on Bypass by Spoofing	10-10-2019	4.3	when impro cooki Brow Vulne uniqu	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357					O-MIC WIND- 22101	-
windows_rt_8	B.1									
Authenticati on Bypass by	10-10-2019	4.3	_	_		ity exists sers doe	I IN / A		O-MIC WIND	
CV Scoring Scal	e 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	De	scription	& CVE II	D	Pa	atch	NCII	PC ID
Spoofing			not prop content, Browser Vulnerat unique fi	aka 'Mica Spoofing pility'. The rom CVE	rosoft g iis CVE -2019-	ID is 1357.			22101	9/516
Improper Restriction of XML External Entity Reference ('XXE')	10-10-2019	9.3	A remote vulnerab Microsof MSXML I input, ak Code Exe	N/A		O-MIC WIND 22101				
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	A remote vulnerable that the handles aka 'VBS Execution CVE ID is 2019-12	N/A		O-MIC WIND 22101				
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	A remote vulnerable Window imprope memory Imaging Executio	N/A		O-MIC WIND 22101				
Improper Privilege Management	10-10-2019	7.2	An eleva vulnerab Window manager hard link Error Re Elevation Vulnerab unique fi	N/A		0-MIC WIND- 22101				
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	l-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		Patch	NCIII	PC ID
			CVE-2	2019-13	42.					
			CVE I	D : CVE-	2019-1	315				
Information Exposure	10-10-2019	4.3	when Secur Exten sessio Windo Secur Vulne	ity (TLS) ded Mas ons, aka ' ows Tra ity Spoo rability'	ort Layer S) accesses non- ster Secret (EMS) 'Microsoft nnsport Layer ofing				O-MIC WIND- 22101	
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1319					A	O-MIC- WIND- 22101	
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	4.9	vulne Windo buffer when impro local o for 32 'Wind Buffer Privilo	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1325					O-MIC- WIND- 22101	•
Improper Input Validation	10-10-2019	7.8	vulne Deskt an att target sends reque	ial of ser rability of op Proto acker co system speciall sts, aka te Deskt	exists in ocol (RD onnects t using R y crafte 'Windov	P) where to the DP and d		Α	O-MIC- WIND- 22101	
CV Scoring Scal (CVSS)	e 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		Pa	itch	NCIII	PC ID
			Vulne	Denial erability' D: CVE-	•						
Improper Input Validation	10-10-2019	9.3	A rem vulne Wind Client a mal 'Remo Remo Vulne	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1333 A spoofing vulnerability exists						O-MIC WIND- 22101	
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357					I/A		O-MIC WIND- 22101	•
windows_serv	ver_2008										
Authenticati on Bypass by Spoofing	10-10-2019	4.3	when not process conte Brow Vulne uniqu	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357. CVE ID: CVE-2019-0608						O-MIC WIND- 22101	
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	vulne that thandlaka 'V Execu CVE II	note code rability of the VBScript of the UBScript of the UBSc	exists in ript engi ts in me Remote nerabili jue from	the way ine mory, Code ty'. This	N	I/A		O-MIC WIND- 22101	
CV Scoring Scal (CVSS)	e 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
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342. CVE ID: CVE-2019-1315	N/A	O-MIC- WIND- 221019/529
Information Exposure	10-10-2019	4.3	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'. CVE ID: CVE-2019-1318	N/A	O-MIC- WIND- 221019/530
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1319	N/A	O-MIC- WIND- 221019/531
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	4.9	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.	N/A	O-MIC- WIND- 221019/532
CV Scoring Scal (CVSS)	e 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
			CVE ID : CVE-2019-1325		
Improper Input Validation	10-10-2019	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. CVE ID: CVE-2019-1326	N/A	O-MIC- WIND- 221019/533
Improper Input Validation	10-10-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1333	N/A	O-MIC- WIND- 221019/534
Information Exposure	10-10-2019	4.3	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'. CVE ID: CVE-2019-1361	N/A	O-MIC- WIND- 221019/535
Information Exposure	10-10-2019	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure	N/A	O-MIC- WIND- 221019/536
CV Scoring Scal (CVSS)	e 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	on & CV	E ID	Р	atch	NCIII	PC ID
			Vulne	rability'.						
			CVE I	D : CVE-	2019-1	363				
windows_serv	ver_2012									
Authenticati on Bypass by Spoofing	10-10-2019	4.3	when not pronte Brows Vulne uniqu	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357. CVE ID: CVE-2019-0608 A remote code execution					O-MIC- WIND- 22101	
Improper Restriction of XML External Entity Reference ('XXE')	10-10-2019	9.3	vulne Micro MSXM input, Code	rability o soft XMI IL parse , aka 'MS Executio	exists w L Core S r proces XML Ro n Vulne	hen the ervices sses user emote erability'	,		O-MIC- WIND- 22101	
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239. CVE ID: CVE-2019-1238				N/A		O-MIC WIND- 22101	
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1311				N/A		O-MIC- WIND- 22101	
Improper Privilege	10-10-2019	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting				N/A		O-MIC- WIND-	
CV Scoring Scal (CVSS)	e 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
Management			manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339 CVE-2019-1342.		221019/541
Information Exposure	10-10-2019	4.3	A spoofing vulnerability exist when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'. CVE ID: CVE-2019-1318		O-MIC- WIND- 221019/542
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles at executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1319	N/A	O-MIC- WIND- 221019/543
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	4.9	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1325		O-MIC- WIND- 221019/544
Improper Input	10-10-2019	7.8	A denial of service vulnerability exists in Remot	e N/A	O-MIC- WIND-
CV Scoring Sca (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		Descript	ion & CV	E ID		Pat	tch	NCIII	PC ID
Validation			an att target sends reque Remo (RDP)	op Proto acker co system speciall sts, aka te Deskt Denial rability'	onnects to using R y crafted 'Window cop Proto of Service	to the DP and dws	1			22101	9/545
			CVE ID : CVE-2019-1326								
Improper Input Validation	10-10-2019	9.3	vulne Winde Client a mali 'Remo Remo Vulne	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1333						O-MIC- WIND- 22101	
Authenticati on Bypass by Spoofing	10-10-2019	4.3	when impro cookid Brows Vulne uniqu	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357						O-MIC- WIND- 22101	
windows_serv	ver_2016										
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357. CVE ID: CVE-2019-0608					N/A		O-MIC- WIND- 22101	
Improper Restriction of XML	10-10-2019	9.3	vulne	ote code rability o	exists w	hen the	N	N/A		0-MIC- WIND- 22101	
CV Scoring Scal (CVSS)	e 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
External Entity Reference			MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.		
('XXE')			CVE ID: CVE-2019-1060		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.	N/A	O-MIC- WIND- 221019/550
			CVE ID : CVE-2019-1238		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366. CVE ID: CVE-2019-1307	N/A	O-MIC- WIND- 221019/551
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366. CVE ID: CVE-2019-1308	N/A	O-MIC- WIND- 221019/552
Improper Restriction	10-10-2019	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC- WIND-
CV Scoring Scal (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	P	atch	NCIII	PC ID				
of Operations within the Bounds of a Memory Buffer			impro memo Imagi Execu	ows Ima operly ha ory, aka ' ng API R ition Vul' D : CVE-	andles o Windov emote (nerabili			22101	9/553					
Improper Privilege Management	10-10-2019	7.2	vulne Wind mana hard l Error Eleva Vulne uniqu CVE-2	Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.				An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342. CVE ID: CVE-2019-1315			N/A		O-MIC WIND- 22101	-
Improper Privilege Management	10-10-2019	7.2	vulne Micro when handl 'Micro Eleva Vulne	evation of rability of soft Windie it does not be common to be considered by the construction of Perability'. D: CVE-	exists in dows So not prop ges, aka ndows S rivilege	etup eerly etup	N/A		O-MIC- WIND- 221019/555					
Improper Link Resolution Before File Access ('Link Following')	10-10-2019	5.6	vulne Wind hard Wind Vulne	ial of ser rability of ows imp links, aka ows Den erability'. D: CVE-	exists w roperly a 'Micro ial of Se	handles soft rvice	N/A		O-MIC WIND- 22101	-				
Information Exposure	10-10-2019	4.3	when Secur Exten session	when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft			A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer			O-MIC- WIND- 221019/557				
CV Scoring Scal (CVSS)	e 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
			Security Spoofing Vulnerability'.		
			CVE ID: CVE-2019-1318		
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1319	N/A	O-MIC- WIND- 221019/558
Improper Authenticati on	10-10-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340. CVE ID: CVE-2019-1320	N/A	O-MIC- WIND- 221019/559
Improper Authenticati on	10-10-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340. CVE ID: CVE-2019-1322	N/A	O-MIC- WIND- 221019/560
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336.	N/A	O-MIC- WIND- 221019/561

Weakness	Publish Date	CVSS		Descripti	ion & CVI	ID		Patch	NCIII	C ID
			CVE I	D : CVE-	2019-1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	4.9	Wind buffer when impro local for 32 'Wind Buffe Privil	vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-1325				A	O-MIC- WIND- 22101	
Improper Input Validation	10-10-2019	7.8	A den vulne Deskt an att target sends reque Remo (RDP) Vulne	ial of ser rability of cop Proto cacker co t system s speciall ests, aka ote Deskt Denial of erability'.	exists in ocol (RD nnects to using Rlaw crafted Window op Proto of Service.	N/A	Α	O-MIC- WIND- 22101		
Improper Input Validation	10-10-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1333				N/1	A	O-MIC- WIND- 22101	
Improper Restriction of Operations within the Bounds of a	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine					Α	O-MIC- WIND- 22101	
CV Scoring Scal	e 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
Memory Buffer			Vulne uniqu CVE-2 1366.	ory Corru rability'. e from C 2019-130 D : CVE-	This CV VE-201 O8, CVE-	9-1307, -2019-				
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323. CVE ID: CVE-2019-1336 An information disclosure						O-MIC WIND 22101	
Information Exposure	10-10-2019	2.1	vulne Windo handl aka 'V Inforr Vulne uniqu	rability of the constant of th	N/A		O-MIC WIND 22101			
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357				N/A		O-MIC WIND 22101	
Improper Restriction of Operations within the Bounds of a	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine				N/A		O-MIC- WIND- 221019/569	
CV Scoring Scal (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
Memory Buffer			Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019- 1335.		
			CVE ID : CVE-2019-1366		
windows_serv	ver_2019	1		T	
Authenticati on Bypass by Spoofing	10-10-2019	4.3	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.	N/A	O-MIC- WIND- 221019/570
			CVE ID: CVE-2019-0608		
Improper Restriction of XML External Entity Reference ('XXE')	10-10-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1060	N/A	O-MIC- WIND- 221019/571
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.1	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239. CVE ID: CVE-2019-1238	N/A	O-MIC- WIND- 221019/572
Improper Restriction of Operations within the Bounds of a Memory	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC- WIND- 221019/573

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Buffer			2019-1238.		
			CVE ID : CVE-2019-1239		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.	N/A	O-MIC- WIND- 221019/574
			CVE ID: CVE-2019-1307		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366. CVE ID: CVE-2019-1308	N/A	O-MIC- WIND- 221019/575
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	9.3	A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'. CVE ID: CVE-2019-1311	N/A	O-MIC- WIND- 221019/576
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows	N/A	O-MIC- WIND- 221019/577
CV Scoring Scal (CVSS)	e 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
			Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.		
			CVE ID : CVE-2019-1315		
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.	N/A	O-MIC- WIND- 221019/578
			CVE ID : CVE-2019-1316		
Improper Link Resolution Before File Access ('Link Following')	10-10-2019	5.6	A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'. CVE ID: CVE-2019-1317	N/A	O-MIC- WIND- 221019/579
Information Exposure	10-10-2019	4.3	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'. CVE ID: CVE-2019-1318	N/A	O-MIC- WIND- 221019/580
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.	N/A	O-MIC- WIND- 221019/581

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1319		
Improper Authenticati on	10-10-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340. CVE ID: CVE-2019-1320	N/A	O-MIC- WIND- 221019/582
Improper Authenticati on	10-10-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340. CVE ID: CVE-2019-1322	N/A	O-MIC- WIND- 221019/583
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336. CVE ID: CVE-2019-1323	N/A	O-MIC- WIND- 221019/584
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	4.9	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of	N/A	O-MIC- WIND- 221019/585
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
			Privilege Vulnerability'.							
			CVE I	D : CVE-	2019-1	325				
Improper Input Validation	10-10-2019	7.8	Deskt an att target sends reque Remo (RDP) Vulne	vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. CVE ID: CVE-2019-1326				A	O-MIC- WIND- 22101	
Improper Input Validation	10-10-2019	9.3	vulne Wind Client a mal 'Remo Remo Vulne	note code rability e ows Rem a icious se ote Desk ote Code erability'.	exists in note Des user con rver, ak top Clien Execution	o N/A	Α	O-MIC- WIND- 22101		
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	vulne that the engin memo 'Chak Memo Vulne uniqu CVE-2 1366.	note code rability of the Chakre e handle ory in Mi ra Script ory Correction Constitution (2019-130).	the way ing s in Edge, ak ine 'E ID is 9-1307, 2019-	xa N/A	A	O-MIC- WIND- 22101		
Improper Privilege Management	10-10-2019	7.2	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka					A	O-MIC- WIND- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	C ID			
			Client Vulne	osoft Wi Elevation Trability' Te from (on of Pri . This CV	vilege Æ ID is							
			CVE I	D : CVE-	2019-1	336							
Information Exposure	10-10-2019	2.1	vulne Wind handl aka 'V Inforr Vulne uniqu	formation rability of the constant of the cons	exists wanel improtes in me served Kernel Disclosure This CV CVE-201	hen the operly mory, re VE ID is 9-1334.	N/A	A	O-MIC- WIND- 22101				
Authenticati on Bypass by Spoofing	10-10-2019	4.3	when improcooking Brow Vulne uniqu	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608. CVE ID: CVE-2019-1357				A	O-MIC- WIND- 22101				
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-10-2019	7.6	vulne that the engin memo 'Chak Memo Vulne uniqu CVE-2	Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.		xa N/A	A	O-MIC- WIND- 22101					
nixos													
nix													
Incorrect Default	09-10-2019	4.6	Nix through 2.3 allows local users to gain access to an				<u> </u>			N/A	A	0-NIX- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
Permissions			becau of the is wo	ary user se the puser-production and writa D: CVE-	arent di ofile dir ıble.					
opengroup										
unix										
Insufficient Verification of Data Authenticity	03-10-2019	5	before platfo about failed easier enum	d/daem e 1.9.1 o rms pro why au , which n for atta erate va D : CVE -	n non-W vides de thentica night m ckers to lid user	Vindows etails tion ake it names.	hub he- tcpc gro cap bpc 1.9, GES http hub he- tcpc gro cap t/4 bf7 8c3 2d6 78c6 http www mp	/CHAN S, os://git o.com/t dump- up/libp /commi 84d60c ca4ec75 cbb8a8 68b244a l58, os://w s.tcpdu org/pu	0-0PE 22101	
Opensuse										
leap										
Improper Neutralizatio n of Special Elements in Output Used	01-10-2019	5	the "b prote may a	Y before pracketed ction meallow a second to the contraction of the co	d paste i echanism ession to	mode" n, which		A	O-OPE LEAP- 22101	
CV Scoring Scal (CVSS)	e 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		Pa	itch	NCIII	PC ID
by a Downstream Component ('Injection')			•	ard con D : CVE-		7068					
Improper Input Validation	01-10-2019	5	remot a deni freed SSH1_ messa	e SSH-1 al of ser memory MSG_DI	servers vice by locatio SCONNI		e ig	I/A		O-OPE LEAP- 22101	
Redhat											
enterprise_lir	nux										
Deserializati on of Untrusted Data	01-10-2019	7.5	vulner discov imple: CVE fi CVE-2 15095 2018- 10008 report jackso imple: appro these future	es of destrabilities vered in mented exes CVE (017-75), CVE-2 (7489, CVE (1489), CVE (1489	s have b Codeha in EAP 7 -2017-1 25, CVE- 018-596 VE-2018 C-2019-1 CasterXM oind by g a white will mire bilities a ike.	een us 1.9.x 7. This 7485, 2017- 68, CVE- 3- 12086 1L elist tigate and	gz at w dz 2	zilla t.co	-	O-RED ENTE- 22101	
socomec											
diris_a-40_fir	mware										
Insufficiently Protected Credentials	09-10-2019	10	Password disclosure in the web interface on socomec DIRIS A-40 devices before 48250501 allows a remote attacker to get full access to a device via the /password.jsn URI.					I/A		0-SOC 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6					7	7-8	8-9	9-10

Weakness	Publish Date	cvss	·					Pa	tch	NCIII	PC ID				
			CVE I	D : CVE-	2019-1	5859									
Suse															
suse_linux_en	terprise_serv	er													
Incorrect Default Permissions	07-10-2019	6.6	packa Linux before 4.8-5. Enter and ir had so perminattack the so persis binary	The /usr/sbin/pinger binary backaged with squid in SUSE binux Enterprise Server 15 before and including version 8.8-5.8.1 and in SUSE Linux Enterprise Server 12 before and including 3.5.21-26.17.1 had squid:root, 0750 bermissions. This allowed an attacker that compromissed the squid user to gain bersistence by changing the binary EVE ID: CVE-2019-3688				ckaged with squid in SUSE ux Enterprise Server 15 ore and including version -5.8.1 and in SUSE Linux terprise Server 12 before d including 3.5.21-26.17.1 d squid:root, 0750 missions. This allowed an acker that compromissed e squid user to gain resistence by changing the ary				zilla om/ oug.	://bu .suse. show cgi?id 3414	0-SUS- 22101	
vzug															
combi-stream	ı_mslq_firmw	are													
Improper Authenticati on	06-10-2019	5	Zug C device and b is no l (e.g., l attack brute authe	ombi-Stes before Wester ockout) ser mightoricate o	eam MS. E Ethern LAN ROS ce prote establis t be able e passwo	LQ net R07 5. There ection whed. An e to ord to evice.	N	//A		O-VZU COMB- 22101	-				
Improper Authenticati on	06-10-2019	7.5	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. Password authentication uses MD5 to hash passwords. Cracking is possible with minimal effort. CVE ID: CVE-2019-17216					/A		O-VZU COMB- 22101	-				
CV Scoring Scal (CVSS)	e 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		Descript	ion & CV	E ID	ı	Patch	NCIII	PC ID
Cross-Site Request Forgery (CSRF)	06-10-2019	6.8	Zug C device and b is no estab	ombi-Stones before With the control of the control	eam MS e Ethern LAN ROS otection n the we	et R07 5. There b service	N/A	L	O-VZU COMB 22101	
Missing Encryption of Sensitive Data	06-10-2019	5	Zug C device and b defau the w via ht interc comm service	ssue was discovered on V-Combi-Steam MSLQ ices before Ethernet R07 before WLAN R05. By mult, the communication to web service is unencrypted attp. An attacker is able to rcept and sniff imunication to the web vice. SID: CVE-2019-17218 ssue was discovered on V-					0-VZU COMB 22101	-
Improper Authenticati on	06-10-2019	5.8	Zug C device and b defau enfor adjace the ne	ombi-Stones before Williams the december any are any are ant attace	eam MS e Ethern LAN ROS evice doo uthentic ker is al nterface control	LQ let R07 5. By es not ation. Ar ole to use without	N/A	1	0-VZU COMB 22101	-
XEN									L	
xen										
Improper Input Validation	08-10-2019	6.1	Xen the x86 g denia privil transf	sue was on rough 4 uest OS of servings become fer requestandled. D: CVE-	1.11.x all users to ice or ga ause gra ests are	owing cause a iin ant-table	N/A	1	0-XEN 22101	-XEN- 9/605
CV Scoring Scal (CVSS)	e 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		Patch	NCII	PC ID
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	08-10-2019	6.9	Xen the x86 PV a deni privile page-V during througe	ue was on ough 4 guest (alof sereges by leadition gaddition gh PCI de CVE-	.11.x all OS users vice or g everagin ty race on of a p evice.	owing to caus gain ng a conditio assed-	N/A	Α	0-XEN 22101	-XEN- 9/606
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	08-10-2019	4.4	Xen the x86 PV a deni privile condit XENM introd	ue was on the was of the was of serieges by letion that the was also become and the was also become also become also become also become also become a was also become and the was also become and the was also become and the was also become also bec	.11.x all OS users vice or g everagin arose w nange w	owing to caus gain ng a race vhen ras		A	0-XEN 22101	
Improper Input Validation	08-10-2019	4.6	Xen the x86 PV a deni privile incorr physm domai	ue was on a rough 4 V guest (alof sereges by left) rect use on a rough. D: CVE-	.11.x all OS users vice or a everagin of the Hi rept for	owing s to caus gain ng VM PV	e N/A	Δ	0-XEN 22101	-XEN- 9/608
Improper Input Validation	08-10-2019	4.9	Xen the x86 PV a deni leveral operate suppound update	ue was on rough 4 y guest (al of sereging a lotion that or trestances.	.11.x all OS users vice by ong-run exists t tability	owing to caus ning to of PTE	e N/A	Λ	0-XEN 22101	-XEN- 9/609
Improper Input	08-10-2019	4.9	An issue was discovered in Xen 4.8.x through 4.11.x allowing x86 PV guest OS					Λ	0-XEN 22101	-XEN- 9/610
CV Scoring Scal (CVSS)	e 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
Validation			users to cause a denial of service because mishandling of failed IOMMU operations causes a bug check during the cleanup of a crashed guest. CVE ID: CVE-2019-17345		
Improper Input Validation	08-10-2019	7.2	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because of an incompatibility between Process Context Identifiers (PCID) and TLB flushes. CVE ID: CVE-2019-17346	N/A	O-XEN-XEN- 221019/611
Improper Input Validation	08-10-2019	4.6	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because a guest can manipulate its virtualised %cr4 in a way that is incompatible with Linux (and possibly other guest kernels). CVE ID: CVE-2019-17347	N/A	O-XEN-XEN- 221019/612
Improper Input Validation	08-10-2019	4.9	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service because of an incompatibility between Process Context Identifiers (PCID) and shadow-pagetable switching. CVE ID: CVE-2019-17348	N/A	O-XEN-XEN- 221019/613
Loop with Unreachable Exit Condition ('Infinite	08-10-2019	4.9	An issue was discovered in Xen through 4.12.x allowing Arm domU attackers to cause a denial of service (infinite loop) involving a LoadExcl or	N/A	O-XEN-XEN- 221019/614
CV Scoring Scal (CVSS)	e 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 & CVI	P	atch	NCIII	NCIIPC ID	
Loop')			Storel	Excl ope	ation.					
			CVE I	D : CVE-	2019-1	7349				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-10-2019	4.9	Xen the Arm denial involves		.12.x all ackers t ce (infir mpare-a ration.	owing to cause a nite loop) and-	-		0-XEN 22101	
Uncontrolled Resource Consumption	08-10-2019	4.9	driver Linux used i allowicause becau resour	ue was or s/xen/be kernel be n Xen the ing guest a denial se of unities of consapping of D-6ef36	alloon.o efore 5. rough 4 OS use of servi restricte umption	N/A		0-XEN 22101		
			CVE I	D : CVE-	2019-1	7351				
Xerox										
atlalink_firm	ware									
Improper Privilege Management	04-10-2019	7.5	B8045 B8090 C8030 C8070 before allow	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.					0-XER ATLA- 22101	
						7104				
Cisco		Hardware								
asa_5505										
Improper Input Validation	02-10-2019	5	insped	nerability ction eng ive Secu	gine of C	lisco	N/A		H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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 & CVI	E ID		Patch	NCIII	PC ID
			Threa Softw unaut attack service affect vulne insuff data. It this v malic an affexplo attack	rare and care could henticate care could care to cause (DoS) ed device rability in attack an attack ious FTP ected device to cause tion on te.	te (FTD) d allow a ed, remander use a descondition e. The s due to lidation ker coul lity by s traffic t vice. A s allow the use a Do	an ote nial of on on an of FTP d exploi ending chrough uccessfue	t			
				D : CVE-						
Improper Input Validation	02-10-2019	3.3	Short imple Adapt (ASA) Firepo (FTD) unaut attack affect denia condi exists softw certai state at 11 pa explo sendir OSPF device could	nerability est Path mentation tive Secu Softwar ower The Softwar chenticat ker to cau ed device I of servi tion. The because are impr n option advertise ckets. Ar it this vu ng a craf packet to a succe allow th a reload	First (O on of Cistrity Appres and Cistrity Appres and Cistrity Appres and Cistrity Appres are could led, adjance a relation of the affect of the affect LSA of an affect attack are	n N/A	A	H-CIS- 22101	_	
CV Scoring Scal (CVSS)	e 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	Р	atch	NCIIF	C ID
			condi is trav	e, resulti tion for oversing t D: CVE-	client tra	affic tha ce.	t			
Improper Handling of Exceptional Conditions	02-10-2019	4	Socker feature Secure Software authorized to cause (DoS) the creation of the creation of the creation of the creation of the after this very local authorized the after which memory session of the creation o	nerability its Layer re of Cisc ity Applitare coul nticated use a den condition reation of ranspor connect ed device rability if rect hand led strin exploit if ening ma ons to an ttacker w valid use fected de ulnerability in exploit if ening ma ons to an ttacker w valid use fected de ulnerability it could a cer to ove m memo a will eve ory alloc is L/TLS e, prever lishment ons. A rel ulred to ondition rLS conn e and SS ections the are not	(SSL) Very Adapt to A	PN cive SA) an e attacker rvice brevents Security an Base64- ctacker herability VPN d device eed to htials on exploit accessful e a specia ion, result in rors for s to the ccessful e he device from shed to the	y N/A		H-CIS-22101	_
CV Scoring Scal (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
			Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions. CVE ID: CVE-2019-12677		
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. CVE ID: CVE-2019-12678	N/A	H-CIS-ASA 221019/621
Incorrect Type Conversion or Cast	02-10-2019	4	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use	N/A	H-CIS-ASA 221019/622
CV Scoring Scal (CVSS)	e 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	Р	atch	NCIII	PC ID
			length could by initiarge via SC vulne would on the succestible at length which device	incorrect n variable exploit to tiating the file to and CP. To exprability, dege level e affected e affected ssful expression variable n could care	e. An att this vulr he trans a affected ploit thi the atta have va d device oloit cou o cause t e to roll ause the h.	tacker herability fer of a d device s cker alid dentials . A ld allow che over,	y			
				D : CVE-		2693				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	Client portal Secur Cisco Defen allow remote cross-attack web-k interf The vinsuff suppl based of an attack vulne user of crafte exploin attack	nerability cless SSL l of Cisco ity Appli Firepow ase (FTD) an unau te attack site scri against cased ma ace of an ulnerabi icient va ied input manage affected rability l of the int ed link. A it could a ace to exe	VPN (We have a Adaption of Ada	ve SA) and at are could ated, induct a SS) of the ent d device ue to of user- web- aterface An athis adding a o click a aful e	n. N/A		H-CIS- 22101	
			the in	terface o						

Weakness	Publish Date	CVSS	Description & CVE ID	Pa	tch	NCIIF	PC ID
			attacker to access sensitive browser-based information.				
			CVE ID : CVE-2019-12695				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.	N/A		H-CIS-22101	_
			CVE ID : CVE-2019-12698				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is	N/A		H-CIS-22101	_
CV Scoring Scal (CVSS)	e 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				Pa	tch	NCIII	PC ID
			due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256								
asa_5510											
Improper Input Validation	02-10-2019	5	inspectade Adapt Softw Threat Softw unaut attack service affect vulne insuff data. It this will malice an affect exploattack conditions and the soft conditions are soft attack conditions and the soft conditions are soft attack conditions are soft attack conditions.	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.				//A		H-CIS 22101	
CV Scoring Scal (CVSS)	e 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		Descript	ion & CVI	E ID		Patch	NCII	PC ID
Improper Input Validation	02-10-2019	3.3	Short imple Adapt (ASA) Firepo (FTD) unaut attack affect denia condirexists softw certain state at 11 parts explored exists could cause device condirect is trav	ter to caused deviced of servition. The because are impropered in option advertise ckets. Are it this vulue a craft packet the A succeallow the a reloade, resulti	First (O on of Cistrity Appres and Circat Define could ded, adjause a relation (DoS) at the affect of the affect LSA of an affect attacked of the affect affect the affect that affect the affect attacked of the affect affect that affect the affect affect the affect affect the affect	sSPF) sco coliance isco ense allow ar cent oad of ar ing in a) ability ected parses PF link- LSA) typ er could ity by type 11 ected kploit er to affected DoS affic that ee.	n N/A	A	H-CIS- 22101	ASA 9/627
Improper Handling of Exceptional Conditions	02-10-2019	4	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents the creation of new SSL/Transport Layer Security (TLS) connections to an affected device. The vulnerability is due to incorrect handling of Base64-					A	H-CIS- 22101	ASA 9/628
CV Scoring Scale (CVSS)	e 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	Pa	atch	NCII	PC ID
			could by op session the afthis view of the afthis connection of the succession o	ening mand tracker walid used fected decented and ser to over memoral will ever allocations. A relations. A relations. A relations to and SSL/TLS eare not ugh this eare not ugh this essul exprability was solved.	this vulnary SSL affected would not be received to allow the erwrite ry location errought to features. Establications L/TLS affected vulnerary locations to feature affected would affect	derability VPN I device. Heed to Intials on Hexploit Hexp				
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an				N/A		H-CIS- 22101	ASA 9/629
CV Scoring Scal (CVSS)	e 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		Pa	tch	NCIII	PC ID
			affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. CVE ID: CVE-2019-12678 A vulnerability in the Secure								
Incorrect Type Conversion or Cast	02-10-2019	4	Copy Adap (ASA) auther to cau (DoS) vulne of an length could by ini large via SO vulne would privil on the succe the at length which	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.				I/A		H-CIS- 22101	
Improper Neutralizatio	02-10-2019	4.3	A vulnerability in the Clientless SSL VPN (WebVPN)			N	I/A		H-CIS- 22101		
CV Scoring Scal (CVSS)	e 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		Descripti	ion & CVI	E ID	Р	atch	NCIII	PC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Secur Cisco Defen allow remote cross- attack web-k interf The v insuff suppl based of an a attack vulne user of crafte exploi attack script the in attack script the in attack	an unaute attack site script against cased marage of an ulnerabilicient valid and affected rability before the interface of a code in a	tance (A ver Three) Softwa thentical er to con pting (X a user of anagement affected lity is du lidation t by the ement in device. A l exploit by persu erface to success allow the ecute ar the cont or allow cess sen d inform	SA) and at at are could ated, and at a SS) of the ent at a device. Le to a of userweb-terface An at this adding a colick a sful e bitrary text of the sitive nation. 2695				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN				N/A		H-CIS- 22101	_
CV Scoring Scale (CVSS)	e 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	Р	atch	NCIIF	PC ID
			HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device. CVE ID: CVE-2019-12698				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interfact of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256	r N/A		H-CIS-22101	_
CV Scoring Scal	e 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
asa_5512-x					
Improper Input Validation	02-10-2019	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device. CVE ID: CVE-2019-12673	N/A	H-CIS-ASA 221019/634
Improper Input Validation	02-10-2019	3.3	A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF linkstate advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by	N/A	H-CIS-ASA 221019/635

3-4

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS		Descripti	on & CVI	ID	Р	atch	NCIII	PC ID
			sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device. CVE ID: CVE-2019-12676 A vulnerability in the Secure							
Improper Handling of Exceptional Conditions	02-10-2019	4	Socker feature Secure Software auther to cau (DoS) the crestal secure incorred could by operate and the after the after the after system which memory secure auther system which memory secure auther system which memory secure s	ets Layer re of Cisc re of Cisc re of Cisc re of Cisc rety Appli rare coulc rare a den condition reation of ranspor connect ed device rability i rect hand ded string exploit t ening ma ons to an ttacker v valid use fected de ulnerabi it could a ker to ove m memo n will eve ory alloca ory alloca se, prever lishment ons. A rel uired to	(SSL) Voladaption Adaption Ada	PN ive SA) an attacker rvice brevents Security an Base64- tacker erability VPN I device. eed to atials on exploit accessful e a special on, result in rors for to the ecessful e the device	N/A		H-CIS- 22101	_
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	CVSS	Description & CVE ID					Patch	NCII	PC ID
				SSL/T device conne device Altho in the succe vulne new S device session		ections L/TLS hrough to affected vulnera N feature bloitation would assessions ing man	to the the d. Note: bility is e, n of this ffect all s to the agemen				
Integer Underflow (Wrap or Wraparound)	02-	-10-2019	5	A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. CVE ID: CVE-2019-12678				n N/A	4	H-CIS- 22101	_
Incorrect Type Conversion	02-	-10-2019	4	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance					A	H-CIS- 22101	ASA 9/638
CV Scoring Scal (CVSS)	e	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	Р	atch	NCIII	PC ID
or Cast			authe to cau (DoS) vulne of an length could by ini large via SC vulne would privil on the succe the at length which device	nticated, ise a den condition rability in variable exploit the total rability, and reed to ege level exfected ssful explacker to variable is variable.	the atta of cause to cause the description of the d	the use ope for a tacker nerability fer of a device s cker alid lentials . A ld allow the over, e affected	7			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	A vuln Client porta Secur Cisco Defen allow remot cross- attack web-k interf The v insuff suppl based of an a attack vulne	nerability less SSL l of Cisco ity Appli Firepow se (FTD) an unau te attack site scri a against based ma ace of an ulnerabi	y in the VPN (We Adaption Adap	VebVPN) ve SA) and at are could ated, aduct a SS) of the ent d device, ue to a of user- web- aterface An athis adding a	N/A		H-CIS- 22101	_
CV Scoring Scale (CVSS)	e 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
Uncontrolled Resource Consumption	02-10-2019	7.8	crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. CVE ID: CVE-2019-12695 A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.	N/A	H-CIS-ASA 221019/640
			CVE ID : CVE-2019-12698		
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an	N/A	H-CIS-ASA 221019/641
CV Scoring Scal (CVSS)	e 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
			unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256		
asa_5515-x					
Improper Input Validation	02-10-2019	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful	N/A	H-CIS-ASA 221019/642

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	Publish Date 02-10-2019	cvss 3.3	exploit could allow the attacker to cause a DoS condition on the affected device. CVE ID: CVE-2019-12673 A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF link-state advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by	Patch N/A	NCIIPC ID H-CIS-ASA 221019/643
			sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition for client traffic that is traversing the device. CVE ID: CVE-2019-12676 A vulnerability in the Secure		
Improper Handling of Exceptional Conditions	02-10-2019	4	Sockets Layer (SSL) VPN feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition that prevents	N/A	H-CIS-ASA 221019/644
CV Scoring Scal (CVSS)	e 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 & CVI	E ID	F	atch	NCII	PC ID
			SSL/T (TLS) affect vulne incorre encode could by op session The arthur which memory device estable session is required this connected is required this connected althories the succession		t Layer ions to a e. The s due to dling of legs. An atchis vulnary SSL affected would nearly location error locations at of these locations locations affected vulnera locations would at sessions ing man	Base64- ctacker derability VPN I device. deed to dials on exploit diccessful e a special ion, result in rors for s to the decessful e the devic from shed to the dilty is e, n of this effect all s to the agement	y l l e			
Integer Underflow (Wrap or	02-10-2019	5	A vuli Initiat	D : CVE - nerability tion Prot ction mo	y in the cocol (SI	Session P)	N/A		H-CIS- 22101	ASA 9/645
Wraparound CV Scoring Scale	e	1.3	Adaptive Security Appliance					7.0	0.0	0.40
(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					atch	NCIII	PC ID
			(ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. CVE ID: CVE-2019-12678							
Incorrect Type Conversion or Cast	02-10-2019	4	A vulne Copy Adapt (ASA) auther to cau (DoS) vulne of an elength could by iniliarge via SC vulne would privile on the	_					H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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 Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	Publish Date 02-10-2019	4.3	which could cause the affected device to crash. CVE ID: CVE-2019-12693 A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary	Patch N/A	H-CIS-ASA 221019/647
Uncontrolled Resource	02-10-2019	7.8	script code in the context of the interface or allow the attacker to access sensitive browser-based information. CVE ID: CVE-2019-12695 A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD)	N/A	H-CIS-ASA 221019/648
Consumption			Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected		221019/648
CV Scoring Scale (CVSS)	e 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 & CVI	E ID	P	atch	NCIII	PC ID
			to exc for a s page r could by ser HTTP specif exploi attack on the denial condit traffic the de		rocessing WebVPN An attace this vulned the condition of t	y a				
Uncontrolled Resource Consumption	02-10-2019	7.8	the device. CVE ID: CVE-2019-12698 A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map						H-CIS- 22101	
				ed to the affected	ingress I device.		e			

Weakness	Publish Date	cvss	Description & CVE ID					Patch	NCIII	PC ID
asa_5520			attack memo a relo	it could a ser to expory reson ad of an D: CVE-	haust sy urces, le affected	stem ading to device.				
			inspe	nerabilit ction en	gine of C	lisco				
Improper Input Validation	02-10-2019	5	Softw Threa Softw unaut attack service affect vulne insuff data. A this vi malici an affe explosi attack condi- device	cive Securare and at Defens are coulchenticated to care (DoS) and device ability in the coulchest of the cou	Cisco Fi se (FTD) d allow ded, remuse a decondition e. The is due to alidation ker coul lity by so traffic to vice. A so allow the use a Do the affect	N/	A	H-CIS- 22101	-	
Improper Input Validation	02-10-2019	3.3	Shortimple Adapt (ASA) Firepo (FTD) unaut attack affect denia condi	nerability est Path mentation Softwar ower The Softwar chenticate ter to car ed device I of servition. The because	First (Oon of Cistrity Appres and Circat Defore could ted, adjactuse a relation (DoS)	SPF) sco pliance isco ense allow and cent oad of a ing in a) ability		A	H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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				Pa	atch	NCIII	PCID
			certai state a 11 pa explos sendin OSPF device could cause device condi is trav	are impron option advertise ckets. And it this vuring a craft packet to allow the areloade, resultition for oversing the corest of the corest open to the corest open	s in OSF ement (I a attacke lnerabil ted LSA o an affe essful ex e attack of the a ng in a I client tra					
Improper Handling of Exceptional Conditions	02-10-2019	4	Socke feature Secure Softwall auther to cause (DoS) the create SSL/T (TLS) affects which will be affected by opposession. The art this will explore attack system which	nerability res Layer re of Cisc ity Appli rare could rare could rate a den condition reation of ranspor connect ed device rability i rect hand exploit t ening ma ons to an ttacker v valid use fected de ulnerabil it could a xer to ove m memon will eve	N/A y		H-CIS 22101			
i i			IIICIII	ory alloca	ation er	rors for				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			new SSL/TLS sessions to the device, preventing successful establishment of these sessions. A reload of the device is required to recover from this condition. Established SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.		
			CVE ID: CVE-2019-12677		
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and	N/A	H-CIS-ASA 221019/653

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			resulting in a crash. CVE ID: CVE-2019-12678		
Incorrect Type Conversion or Cast	02-10-2019	4	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash. CVE ID: CVE-2019-12693	N/A	H-CIS-ASA 221019/654
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-	N/A	H-CIS-ASA 221019/655
CV Scoring Scal	e 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						itch	NCIII	PC ID
			based of an attack vulne user of crafted explo attack script the in attack brows	ied input manage affected refected rability b of the int d link. A it could a cer to exe code in terface of xer to acc ser-base D: CVE-	ement in device. I exploit oy persuerface to success allow the control or allow cess send information.	An this ading a click a sful e bitrary text of the sitive nation.					
Uncontrolled Resource Consumption	02-10-2019	7.8	feature Secure Software Threat Software Individual CPU with device to except for a secure HTTP specific explorattack on the denial condition of the condition o	A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device.				N/A		H-CIS- 22101	
Uncontrolled	02-10-2019	7.8	A vulnerability in the Internet				N/A		H-CIS-	ASA	
CV Scoring Scale (CVSS)	e 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
Resource Consumption			(IKEV Adapt (ASA) Firepo (FTD) unaut attack an aff a den condi due to of sys could by sen traffic The a valid authe nor de addre stater applie of the explo attack memo a relo	xchange tive Secu- Softwar ower Th Softwar chenticat ker to tri ected de ial of ser tion. The o improp- tem mer exploit ading ma c to an af ttacker of credenti- enticate to oes the a ess need ment in the eaffected it could a ker to ex	e version re of Cisurity Appres and Coreat Defered, remained wice, reservice (Doe vulner ber manathis vulnations of the VPN attacker's to matche cryptic ingress I device, allow the haust synces, le affected aff	cooliance iscooliance iscooliance allow arote eload of sulting iros) ability is agement attacked erability. IKEv1 levice. In eneed session, is source to map interfact An evice ading to device.	n n er y			19/657
asa_5525-x										
Improper Input Validation	02-10-2019	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The				N/A			-ASA 19/658
CV Scoring Scal	e 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					Pa	tch	NCIII	PC ID
			insuff data. this v malic an aff explo attack condi device	rability if icient vach attacleulong FTP ected de ter to caution on terms. D: CVE-	lidation ker coul lity by s traffic vice. A s allow th use a Do he affec	of FTP d exploi ending through successfi e e oS					
Improper Input Validation	02-10-2019	3.3	Short imple Adapt (ASA) Firep (FTD) unaut attack denia condi exists softw certain state 11 particular exploration (ASA)	nerability est Path mentation Softwar Ower The Softwar Chenticate ed device I of service tion. The because are imprended overtise ckets. Ar it this vur ing a craft packet te e. A succe allow the a reload e, resulti tion for oversing te Versing te Versing te CVE-	First (Oon of Cistrity Applete and Core	sco pliance isco fense allow as icent load of a ting in a f) ability ected parses PF link- LSA) typ er could lity by type 11 ected xploit xer to affected DoS affic tha ce.	an De	N/A		H-CIS- 22101	_
Improper Handling of	02-10-2019	4	A vulnerability in the Secure Sockets Layer (SSL) VPN]	N/A		H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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
Exceptional			feature of Cisco Adaptive		
Conditions			Security Appliance (ASA)		
			Software could allow an		
			authenticated, remote attacker		
			to cause a denial of service		
			(DoS) condition that prevents		
			the creation of new		
			SSL/Transport Layer Security		
			(TLS) connections to an		
			affected device. The		
			vulnerability is due to		
			incorrect handling of Base64-		
			encoded strings. An attacker		
			could exploit this vulnerability		
			by opening many SSL VPN		
			sessions to an affected device.		
			The attacker would need to		
			have valid user credentials on		
			the affected device to exploit		
			this vulnerability. A successful		
			exploit could allow the		
			attacker to overwrite a special		
			system memory location,		
			which will eventually result in		
			memory allocation errors for		
			new SSL/TLS sessions to the		
			device, preventing successful		
			establishment of these		
			sessions. A reload of the device		
			is required to recover from		
			this condition. Established		
			SSL/TLS connections to the		
			device and SSL/TLS		
			connections through the		
			device are not affected. Note:		
			Although this vulnerability is		
			in the SSL VPN feature,		
			successful exploitation of this		
			vulnerability would affect all		
			new SSL/TLS sessions to the		
			device, including management		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			sessions. CVE ID : CVE-2019-12677		
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. CVE ID: CVE-2019-12678	N/A	H-CIS-ASA 221019/661
Incorrect Type Conversion or Cast	02-10-2019	4	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this	N/A	H-CIS-ASA 221019/662
CV Scoring Scale (CVSS)	e 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	P	atch	NCIII	PCID	
			would privil on the succe the at length which device	rability, I need to ege level e affected ssful exp tacker to n variabl n could co e to crasi D: CVE-	have various have various 15 created to couse to roll ause the	alid dentials a. A ald allow the over, e affected	ì			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	Client porta Secur Cisco Defendallow remore cross-attack web-kinterf The vinsuff supplicated of an attack vulne user of crafte exploattack script the in attack brows	nerability cless SSL l of Cisco ity Appli Firepow se (FTD) an unau te attack site scri against based ma ace of an ulnerabi icient va ied input manage affected are could rability l of the int ed link. A it could a acer to exe code in terface of acr to acc ser-base D: CVE-	VPN (We had a ptilate of the ntical er to compting (Xe an agental affected by the ement in device. It exploit by persuerface the control of t	ve .SA) and .at .are could .ated, .nduct a .SS) .of the .ent .d device .ue to .a of userwebaterface .An .athis .ading a .o click a .oful .e .bitrary .text of .the .sitive .nation.			H-CIS- 22101	_
Uncontrolled Resource	02-10-2019	7.8	A vuli	nerabilit	y in the	WebVPN	N/A		H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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 & CVI	ID .	Р	atch	NCIII	PC ID
Consumption			Softw Threa Softw unaut attack CPU u device to exc for a s page i could by sei HTTP specif explo attack on the denia condi traffic the de	ity Applicare and out Defense are could thenticate are to cause the receive property of the total are to incompany of the total are to incompany of the total are tota	Cisco Fine (FTD) de allow a ded, remouse incressing WebVPN An attact this vulnultiple Web and request allow the crease Claresulting ich could belayed the could be a succession of the coul	,				
Uncontrolled Resource Consumption	02-10-2019	7.8	Key E (IKEV Adapt (ASA) Firepo (FTD) unaut attack an aff a dent condi due to of sys could by sen traffic	nerability xchange 1) feature Securia Softwar The Softwar Chenticate to triple tend de ial of sertion. The Exploit of the triple to an aftacker of triple to an aftacker of triple tend mere to an aftacker of the triple to an aftacker of the triple to an aftacker of the triple tend mere to an aftacker of the triple triple to an aftacker of the triple t	version re of Ciso rity App re and Ci reat Defo re could red, remo gger a re vice, res vice (Do e vulnera per mana mory. An this vuln fected d	1 co co cliance csco ense allow an ote eload of ulting in ability is agement attacke erability (KEv1 evice.	N/A		H-CIS- 22101	
CV Scoring Scale	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pul	blish Date	cvss		Descript	ion & CV	ı	Patch	NCIII	PC ID	
				authenor de addres stater applie of the exploattack memora a relo	credention ticate to the a affected it could a cours resort and of an D : CVE-	he VPN attacker' to match he crypt ingress I device. allow th haust sy urces, le affected	s source h a peer to map interfac An e stem ading to I device.	ce			
asa_5550											
Improper Input Validation	02-	-10-2019	5	inspe Adapt Softw Threa Softw unaut attack service affect vulne insuff data. this v malic an aff explo attack condi-	nerabilit ction engitive Securare and at Defense coulchenticate (DoS) ed device (DoS) ed device ability in the cted device to cartion on the c.	gine of Carity (AS Cisco Fise (FTD) d allow ted, remuse a decondition is due to didation ker could lity by so allow thuse a Doche affect	cisco A) repower an ote nial of on on an of FTP d exploi ending chrough cuccessfue S ted	N/A		H-CIS- 22101	_
Improper Input Validation	02-	-10-2019	3.3	Short imple Adapt (ASA)	nerabilit est Path mentati tive Secu Softwan	First (O on of Cis crity App re and C	SPF) sco oliance isco	N/A	1	H-CIS- 22101	
CV Scoring Scal	е	0-1	1-2	2-3					7-8	8-9	9-10

Weakness	Publish Date	cvss		Descript	ion & CV	P	atch	NCIII	PCID	
			unaut attack affect denia condi exists softw certai state a 11 pa explo sendia OSPF device could cause device condi is trav	Software chenticated deviced deviced deviced to servition. The cause are improposed are improposed to the cause allow the cause allow the cause are improposed to the cause are improved	ted, adja use a rel e, result ice (DoS e vulnera e the affe roperly p as in OSF ement (I n attacke ulnerabil ted LSA o an affe essful ex e attacke l of the a ng in a I client tra	1				
Improper Handling of Exceptional Conditions	02-10-2019	4	A vuln Socke featur Secur Softw authe to cau (DoS) the cr SSL/T (TLS) affect vulne incorr encod could by op session The a	nerability tes Layer re of Cisc ity Appli rare coul- nticated reation o ranspor connect ed devic rability i rect hand	y in the (SSL) Vec Adapt iance (Adapt iance (Adapt iance (Adapt iance iance is a contract in the is due to iance is any SSL affected would not it is a contract in the iance is any SSL affected would not in the iance is any SSL affected would not in the iance is any SSL affected would not in the iance is any SSL affected would not in the iance is any SSL affected would not in the iance is any SSL affected would not in the iance is a contract in the i	Secure PN cive SA) an e attacker rvice brevents Security an Base64- ctacker herability VPN d device. eed to	N/A		H-CIS- 22101	_
CV Scoring Scal (CVSS)	e 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	P	atch	NCIII	PC ID
			this viexplorattack system which memore stable session is required this connection of the succession o	it could a ker to over m memon will ever ory allocates Est/TLS e, prever lishment ons. A reludition fLS connumered to ondition fLS connumered to eare not ugh this estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the estions the	lity. A suallow the erwrite ry location errors at location errors the cover and of the cover affected would at sessions ing man	a special ion, result in rors for to the ccessful e he device from shed to the bility is e, n of this ffect all to the agement				
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	Initiation inspections (ASA) Firepo (FTD) unaut attack service affect vulne impromessa explore	chenticat ker to cau ce (DoS) ed devic rability i oper pars ages. An it this vu	cocol (SI odule of crity Appres and Ci reat Def ce could ded, removes use a de- condition e. The is due to sing of S attacker	P) Cisco cliance isco ense allow an ote nial of on on an IP could	N/A		H-CIS- 22101	
CV Scoring Scale (CVSS)	e 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	P	atch	NCII	PC ID	
Incorrect Type Conversion or Cast	02-10-2019	4	the at integer software unmare result CVE II A vulra Copy Adapt (ASA) auther to caural (DoS) vulner of an integer via SC vulner would privile	successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. CVE ID: CVE-2019-12678 A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A					H-CIS- 22101	ASA
			length which device CVE I	e to crasl D : CVE-	e to roll ause the h. 2019-1	over, affected				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	Client portal Secur Cisco Defen allow	of Cisco ity Appli Firepow	VPN (Wood Adaption Ad	SA) and at are could ated,	N/A		H-CIS- 22101	
CV Scoring Scale (CVSS)	e 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	NCIII	PC ID
			attack web-k interf The v insuff suppl based of an attack vulne user of crafte exploattack script the in attack brows	rsite script against cased made of an ulnerabilicient valid inpublication and affected affected affected in terface of a code in terfac	a user of anagement affected lity is dualition to by the ement in device. A lexploit by persurerface to success allow the control affect for allow cess send information affects.					
Uncontrolled Resource Consumption	02-10-2019	7.8	A vuln featur Secur Softw Threa Softw unaut attack CPU u device to except for a spage recould by sen HTTP specific exploattack on the	nerability re of Cisconity Applicate and at Defense could be recorded to the care to cause the could appear to inconity and a great to inconity and a	y in the co Adapt ance (A Cisco Fire (FTD) d allow ed, remuse incresing on an allorability occasion. WebVPN An attact this vulrultiple Web ad request allow the crease C resulting to A success allow	WebVPN ive SA) repower an ote eased affected lity is du g load HTTP eker herability vebVPN ests for a sful e PU load	e N/A		H-CIS- 22101	
CV Scoring Scale (CVSS)	e 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	P	atch	NCII	PC ID	
			traffic the de	D : CVE-	elayed tl 2019-1	hrough				
Uncontrolled Resource Consumption	02-10-2019	7.8	(IKEV) Adapt (ASA) Firepo (FTD) unaut attack an affe a deni condit due to of syst could by sen traffic The at valid of auther nor do addres staten applie of the exploi attack memo a reloa	henticated to trige ected devial of servicion. The improper men men exploit to an affect device the asserved of the affect educate to the affect educate to exploit the affect educate to exploit and the affect educate to exploit and the exploit affect educate to exploit and the exploit	re of Cis rity App re and C reat Def re could ed, rem gger a re vice, res vice (Do e vulner er mana his vulr elicious fected d loes not als to he VPN ttacker' to match he crypt ingress device. allow th naust sy arces, le affected	co coliance isco fense allow an ote eload of sulting in oS) ability is agement attacke nerability IKEv1 levice. aneed session, s source h a peer to map interface An e estem ading to I device.	r N/A		H-CIS- 22101	ASA 9/673
asa_5555-x			T						T	
Improper Input Validation	02-10-2019	5	inspec Adapt Softwa	erability ction eng ive Secu are and (t Defens	gine of (rity (AS Cisco Fi	Cisco (A) repower	N/A		H-CIS- 22101	ASA 9/674
CV Scoring Scale (CVSS)	e 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	Р	atch	NCIII	PC ID	
			unaut attack service affecte vulne insuff data. A this ve malice an affe explose attack condi- device		ed, remuse a decondition of the could be affect of the affect of the could be could	t				
			A vulr	nerability	y in the	Open				
Improper Input Validation	02-10-2019	3.3	A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF linkstate advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by sending a crafted LSA type 11 OSPF packet to an affected device. A successful exploit could allow the attacker to cause a reload of the affected						H-CIS- 22101	
				e, resulti tion for o	_		t			

Weakness	Publish Date	cvss	Description & CVE ID					atch	NCIIF	PC ID
			is trav	ersing t	he devi	ce.				
			CVE I	D : CVE-	2019-1	2676				
Improper Handling of Exceptional Conditions	02-10-2019	4	Socker feature Secure Software authorized to cau (DoS) the crest SSL/T (TLS) affect vulner incorred could by opposession The art this vexploattack system which memory session is required this crest system of the could be session in the crest system of the crest syst	nerability its Layer re of Cisc ity Appli are coul inticated ise a den condition canspor connect ed devic rability in rect hand led string mins to an ttacker w valid use fected de ulnerability could a cer to ove memon will ever lishment ons. A rel uired to ondition CLS conn e and SSI ections the are not ugh this SSL VPN	(SSL) Veo Adapted ance (Adalow and allow and allow and ance (Adalow and ance (Adalow and ance (Adalow ance (Adaoo (Adaoo (Adaoo (Adaoo (Adaoo (Adaoo (Adaoo (Adaoo (Adaoo (Ada	PN ive SA) an attacke rvice brevents Security an Base64- ctacker aerability VPN device. eed to attacker aerability incessful e a special ion, result incressful e the device from shed to the che che che che che che che che che c	y N/A		H-CIS- 22101	_
CV Scoring Scal	e 0-1	1-2	2-3		4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions. CVE ID: CVE-2019-12677		
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash. CVE ID: CVE-2019-12678	N/A	H-CIS-ASA 221019/677
Incorrect Type Conversion or Cast	02-10-2019	4	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker	N/A	H-CIS-ASA 221019/678
CV Scoring Scale (CVSS)	e 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
			could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash. CVE ID: CVE-2019-12693		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user- supplied input by the web- based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive	N/A	H-CIS-ASA 221019/679

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			browser-based information.		
			CVE ID : CVE-2019-12695		
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the WebVPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for a specific WebVPN HTTP page request. An attacker could exploit this vulnerability by sending multiple WebVPN HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device. CVE ID: CVE-2019-12698	N/A	H-CIS-ASA 221019/680
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management	N/A	H-CIS-ASA 221019/681
CV Scoring Scal (CVSS)	e 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 system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256		
asa_5580					
Improper Input Validation	02-10-2019	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device. CVE ID: CVE-2019-12673	N/A	H-CIS-ASA 221019/682

Weakness	Publish Date	cvss		Descript	on & CVI	E ID		Patch	NCII	PC ID
Improper Input Validation	02-10-2019	3.3	Short imple Adapt (ASA) Firepo (FTD) unaut attack affect denia condirexists softw certain state at 11 parts explored exists could cause device condirect is trav	nerability est Path mentation Software Software Software henticate ded device of service tion. The because are impreneration advertise ckets. Are it this vue ang a craft packet to a reload e, resulti tion for of versing to	First (On of Cison of	n N/A		H-CIS- 22101	ASA 9/683	
Improper Handling of Exceptional Conditions	02-10-2019	4	Socke featur Secur Softw authe to cau (DoS) the cr SSL/T (TLS) affect vulne	nerability ts Layer re of Cisc ity Appli are coul nticated conditio eation o ranspor connect ed devic rability i	(SSL) Visco Adapticance (Allow a premote ial of section that premote it Layer is ions to a general to the state of the sta	PN ive SA) an attacke rvice orevents Security	N/A		H-CIS- 22101	ASA 9/684
CV Scoring Scal	e 0-1	1-2	2-3		4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descript	ion & CVI	E ID	Pa	atch	NCII	PC ID
			could by op session the afthis view of the afthis connection of the succession o	ening mand tracker walid used fected designated and ser to over allocated for allocated for allocated for allocated for allocated for and SSL/TLS eare not ugh this eare not ugh this essul exprability was allocated for allocate	this vulnary SSL affected would not be received to allow the erwrite ry location errought to features. Establications L/TLS affected vulnerary locations to feature affected would affect	derability VPN I device. Heed to Hitals on Hit				
Integer Underflow (Wrap or Wraparound)	02-10-2019	5	Initiations in special (ASA) Firepo (FTD) unaut attack	nerability tion Prote tive Secu Softwar ower The Softwar chenticat te (DoS)	tocol (SI dule of drity Appre and Ci reat Def re could ted, remouse a dec	P) Cisco cliance isco ense allow an ote nial of	N/A		H-CIS- 22101	ASA 9/685
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	·					Patch	NCIII	PC ID
			vulne impro messa explo sendi throu succe the at intege softw unma result	ed device rability in per parsenges. An it this vuring a male soful expectacker to tracker under are to tracker under a	s due to sing of S attacker alnerabil icious S fected do oloit cou o trigger flow, car y to reac emory a crash.	IP could lity by IP packe evice. A ld allow an using the d				
Incorrect Type Conversion or Cast	02-10-2019	4	Copy Adapt (ASA) authe to cau (DoS) vulne of an lengtl could by ini large via SC vulne would privil on the succe the at lengtl	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash.				A	H-CIS- 22101	
Improper Neutralizatio	02-10-2019	4.3	A vulnerability in the Clientless SSL VPN (WebVPN)			N/A	A	H-CIS- 22101		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

n of Input									
During Web Page Generation ('Cross-site Scripting')		Secur Cisco Defen allow remote cross- attack web-k interfi The verinsuff supple based of an a attack vulne user of crafte exploit attack script the in attack brows	of Ciscolity Appli Firepowerse (FTD) an unaute attack esite script against acce of an allower ability land inpuration of the intermediate of the i	tance (Alver Three) Software thentical er to conpting (X a user of an agement in device. All exploit by persuerface to success allow the context or allow cess sent d information.	sA) and at re could at ted, aduct a SS) of the ent device to of user-web-terface An this ading a click a ful e bitrary text of the sitive nation.				
Uncontrolled Resource Consumption	019 7.8	featur Secur Softw Threa Softw unaut attack CPU u device to exc for a s page 1 could	nerability re of Cisc ity Appli are and it Defens are coul henticat ter to cau tilization e. The vu essive p specific V request. exploit to	co Adapt lance (Al lisco Fin le (FTD) d allow le led, reme luse incre n on an a llnerabil rocessin WebVPN An attac	ive SA) repower an ote eased affected ity is du g load HTTP eker	. N/A	1	H-CIS 22101	_
				•					

Weakness	Publish Date	CVSS	Description & CVE ID	Р	atch	NCIIF	PC ID
			HTTP page load requests for a specific URL. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition, which could cause traffic to be delayed through the device. CVE ID: CVE-2019-12698				
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256	N/A		H-CIS-22101	_
CV Scoring Scal	e 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
asa_5585-x					
Improper Input Validation	02-10-2019	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of FTP data. An attacker could exploit this vulnerability by sending malicious FTP traffic through an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device. CVE ID: CVE-2019-12673	N/A	H-CIS-ASA 221019/690
Improper Input Validation	02-10-2019	3.3	A vulnerability in the Open Shortest Path First (OSPF) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software improperly parses certain options in OSPF linkstate advertisement (LSA) type 11 packets. An attacker could exploit this vulnerability by	N/A	H-CIS-ASA 221019/691

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Descript	ion & CV	E ID		Patch	NCIII	PC ID
			OSPF device could cause device condi	ng a craft packet to e. A succe allow the a reloace, resultition for versing to EVE-	o an afferestul extended attack lof the anglin a I client transfered to the device the second and the device t					
Improper Handling of Exceptional Conditions	02-10-2019	4	Socker feature Secure Software authors to cau (DoS) the create system incorrection of the authors which memory session attack system which memory session sess	nerability its Layer re of Cisconity Appliare could inticated as a denication of Cransport connected device rability it rect handled string mons to an attacker walld use fected device to own memoral will ever to own. A religious A religious A religious A religious and the control of the control	(SSL) Veo Adapted iance (Adapted iance (Adapted iance (Adapted iance (Adapted iance	PN cive SA) an e attacker rvice brevents Security an Base64- ctacker herabilit VPN d device eed to htials on exploit uccessfu e a specia ion, result in rors for s to the ccessful e the device	y N/A	A	H-CIS- 22101	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pul	blish Date	cvss	Description & CVE ID					Patch	NCIII	PC ID			
				device conne device Altho in the succe vulne new S device session	SSL/TLS connections to the device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.			device and SSL/TLS connections through the device are not affected. Note: Although this vulnerability is in the SSL VPN feature, successful exploitation of this vulnerability would affect all new SSL/TLS sessions to the device, including management sessions.						
Integer Underflow (Wrap or Wraparound)	02-	-10-2019	5	CVE ID: CVE-2019-12677 A vulnerability in the Session Initiation Protocol (SIP) inspection module of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a malicious SIP packet through an affected device. A successful exploit could allow the attacker to trigger an integer underflow, causing the software to try to read unmapped memory and resulting in a crash.					A	H-CIS- 22101	_			
Incorrect Type Conversion	02-	-10-2019	4	A vulnerability in the Secure Copy (SCP) feature of Cisco Adaptive Security Appliance					Α	H-CIS- 22101	ASA 9/694			
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6 6-7 7-8 8-9 9						

Weakness	Publish Date	CVSS		Descripti	ion & CV	ı	Patch	NCIII	PC ID	
or Cast			(ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to the use of an incorrect data type for a length variable. An attacker could exploit this vulnerability by initiating the transfer of a large file to an affected device via SCP. To exploit this vulnerability, the attacker would need to have valid privilege level 15 credentials on the affected device. A successful exploit could allow the attacker to cause the length variable to roll over, which could cause the affected device to crash. CVE ID: CVE-2019-12693							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	02-10-2019	4.3	A vulnerability in the Clientless SSL VPN (WebVPN) portal of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user- supplied input by the web- based management interface of an affected device. An attacker could exploit this vulnerability by persuading a				N/A		H-CIS- 22101	-
CV Scoring Scale (CVSS)	e 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 & CVI	E ID	Р	atch	NCII	PC ID
Uncontrolled Resource Consumption	02-10-2019	7.8	explorattack script the in attack brows CVE I A vuln featur Secur Softw unaut attack CPU undevice to except for a sepage recould by ser HTTP specific explorattack on the denial conditing traffic	d link. A it could a ser to exe code in terface of ser-based by the could at Defense are coul	success allow the coute are the contour allow cess send information and allow ed, remaise increase in coessing VebVPN An attact this vulnatiple Wad request allow the crease Caresulting ce (DoS) ich could be allowed and request allow the crease Caresulting ce (DoS) ich could be allowed and request allow the crease Caresulting ce (DoS) ich could be allowed and request allowed allowed and request allowed and request allowed and request allowed and request allowed allowed allowed and request allowed allow	ful e bitrary ext of the sitive nation. 2695 WebVPN ive SA) repower an ote eased affected ity is due g load HTTP eker erability /ebVPN ests for a sful e PU load eg in a) d cause	e N/A		H-CIS-	
firepower_93	00		CVEI	D: CVE-	2019-1	2090				
			Multi	ple vulne	erabilitie	es in the				
Improper Encoding or Escaping of Output	02-10-2019	7.2	multi- Firepo (FTD) authe	denial of service (DoS) condition, which could cause traffic to be delayed through the device. CVE ID: CVE-2019-12698 Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their					H-CIS- 22101	
CV Scoring Scale (CVSS)	e 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
			FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.		
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other	N/A	H-CIS-FIRE- 221019/698

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			running FTD instances.		
			CVE ID : CVE-2019-12675		
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-FIRE- 221019/699
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	H-CIS-FIRE- 221019/700
Improper Input Validation	02-10-2019	7.2	Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including	N/A	H-CIS-FIRE- 221019/701

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges. CVE ID: CVE-2019-12699 A vulnerability in the		
Uncontrolled Resource Consumption	02-10-2019	6.8	configuration of the Pluggable Authentication Module (PAM) used in Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, and Cisco FXOS Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system. CVE ID: CVE-2019-12700	N/A	H-CIS-FIRE- 221019/702
firepower_41	15				

Weakness	Publish Date	cvss		Descripti	ion & CVI	EID	P	atch	NCIII	PC ID
Improper Encoding or Escaping of Output	02-10-2019	7.2	multi- Firepo (FTD) authe escap FTD in comm privile name: vulne insuff under attack vulne critica filesys could execu privile name: the at runni	ple vulned instance ower This ower This ower This ower the correct ower the control of the comment of the comme	e feature reat Define could a local at a loc	e of Cisco ense allow ar stacker to for their cute e to as on the . An these difying derlying al exploi er to ith root nost d allow other s.	N/A		H-CIS- 22101	
Improper Encoding or Escaping of Output	02-10-2019	7.2	multi- Firepo (FTD) authe escap FTD in comm privile name: vulne insuff under attack vulne critica	ple vulne instance ower Thi Softwar nticated, e the cor nstance a nands wi eges in the space. The rabilities icient pre- clying files ar could rabilities al files or stem. A s	e feature reat Def re could , local at atainer f and exec th root he host he se s are due otection esystem l exploit s by moon a the und	e of Cisco ense allow ar tacker to for their cute e to as on the . An these difying derlying	N/A		H-CIS- 22101	
CV Scoring Scal	le 0-1	1-2	2-3			F-52	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID		Pato	ch	NCIII	PC ID
			execu privilename the at	space. T tacker to ng FTD i	nands whin the lining the line	ith root nost d allow c other s.					
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	Firepoware Determenticater to by are and nd RAR informarabilities n of this	ver Systemention Er ed, rem pass cor File Poli file type tion about s, see the	em ote ofigured cies for es. For out these e Details	N,	/A		H-CIS- 22101	
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	Firepow are Dete allow an chenticat ter to by are and nd RAR informa rabilities n of this	ection Er ection Er ed, rem pass cor File Poli file type tion abo s, see the	em ngine ote nfigured cies for es. For out these e Details	N,	/A		H-CIS- 22101	
firepower_41	25										
Improper Encoding or Escaping of Output	02-10-2019	7.2	(ETD) Software could allow an N/A		rted, remote rpass configured File Policies for file types. For ation about these es, see the Details advisory. -2019-12696 erabilities in the ver System ection Engine n ted, remote rpass configured File Policies for file types. For ation about these es, see the Details advisory. -2019-12697 erabilities in the e feature of Cisco areat Defense re could allow an d, local attacker to ntainer for their		H-CIS- 22101				
CV Scoring Scal (CVSS)	e 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
			commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12674		
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances.	N/A	H-CIS-FIRE- 221019/708

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & 0	CVE ID	P	atch	NCIII	PC ID
			CVE ID : CVE-2019	-12675				
Improper Input Validation	02-10-2019	5	Multiple vulnerabile Cisco Firepower Syst Software Detection could allow an unauthenticated, re attacker to bypass of Malware and File Po RTF and RAR file ty more information a vulnerabilities, see section of this advis	Engine mote onfigured olicies for pes. For bout these the Details ory.	N/A		H-CIS- 22101	
Improper Input Validation	02-10-2019	5	Multiple vulnerability Cisco Firepower Systemare Detection could allow an unauthenticated, reattacker to bypass of Malware and File Port RTF and RAR file tymore information a vulnerabilities, see section of this advise CVE ID: CVE-2019	N/A		H-CIS- 22101		
firepower_41	45				<u> </u>			
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilimulti-instance feature Firepower Threat D (FTD) Software could authenticated, local escape the containerabilities and excommands with room privileges in the homamespace. These vulnerabilities are consufficient protections.	red, remote pass configured File Policies for file types. For tion about these s, see the Details advisory. 2019-12697 Perabilities in the e feature of Cisco reat Defense re could allow an , local attacker to a tainer for their and execute th root he host hese s are due to rotections on the			H-CIS- 22101	
CV Scoring Scal	le 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Pu	blish Date	e CVSS		Descript	ion & CV	E ID	F	atch	NCIII	PCID
				attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12674 Multiple vulnerabilities in the							
Improper Encoding or Escaping of Output	02-	-10-2019	7.2	multi Firep (FTD) authe escap FTD i comm privil name vulne insuff under attack vulne critica filesy could execu privil name the at runni	ple vulne- instance ower The Software naticated e the constance nands with eges in the space. The rabilities ficient propertying file ficient propertying file for could rabilities al files or allow the te commeges with space. The tacker to ng FTD in D: CVE-	e feature reat Def re could , local at ntainer f and exec ith root he host he se s are du cotection esystem d exploit s by moo n the un successf ne attack nands w hin the l his could o impact instance	e of Cisco fense allow as tracker to for their cute e to ns on the . An these difying derlying ul explo ter to ith root nost d allow t other s.	o n n n n n n n n n n n n n n n n n n n		H-CIS- 22101	
Improper Input Validation	02-	-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote				N/A		H-CIS-FIRE- 221019/713	
CV Scoring Scal (CVSS)	e	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		Patch	NCIIF	PC ID
			Malwa RTF a more vulne sectio	ter to by are and I nd RAR informa rabilities n of this D : CVE-	File Poli file type tion abo s, see the advisor	cies for s. For ut these Details y.				
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	ple vulne Firepow are Dete allow ar chenticat er to by are and I nd RAR informa rabilities n of this	ection Er ection Er ed, reme pass cor File Poli file type tion abo s, see the advisor	em ote ofigured cies for s. For ut these e Details	N/.	A	H-CIS-1 22101	
firepower_41	10									
Improper Encoding or Escaping of Output	02-10-2019	7.2	multi- Firepo (FTD) authe escap FTD in comm privile name vulne insuff under attack vulne critica filesys could	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root		n o N/A	A	H-CIS-1 22101		
CV Scoring Scal (CVSS)	e 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 Encoding or Escaping of Output	02-10-2019	7.2	namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12674 Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675	N/A	H-CIS-FIRE- 221019/716
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.	N/A	H-CIS-FIRE- 221019/717

Weakness	Publish Date	CVSS		Descript	ion & CV	E ID	F	atch	NCIII	PC ID
			CVE I	D : CVE-	2019-1	2696				
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697					H-CIS- 22101	
firepower_41	20		CVEI	D: CVE-	2019-1	2097				
Improper Encoding or Escaping of Output	02-10-2019	7.2	multi Firep (FTD) authe escap FTD i comn privil name vulne insuff under attack vulne critica filesy could execu privil name the at runni	ple vulner instance ower The Software inticated e the constance in ands with space. The could rabilitie al files or stem. As allow the commeges with space. The commeges with space. The commeges with space of the commeges with space of the commeges with space. The commeges with space of the comment of t	e feature reat Define could a local at a local at and execution he host the seare due to tection esystem I exploit as by moon the unsuccessful ands within the I his could be impact instance	e of Cisco ense allow an stacker t for their cute e to as on the . An these difying derlying all exploiter to ith root nost d allow t other s.	n o N/A		H-CIS- 22101	
Improper	02-10-2019	7.2	Multi	ple vulne	erabilitio	es in the	N/A	<u> </u>	H-CIS-	FIRE-
CV Scoring Scal (CVSS)	e 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	atch	NCIII	PC ID
Encoding or Escaping of Output			Firepo (FTD) auther escape FTD is common privile name vulne insuffunder attack vulne critical filesystems could execut privile name the attrunni	-instance ower The Softwar nticated e the constance nands wite eges in the space. The rabilities of the comment	reat Define could a local at and exemple the host the host the seare dure to the exploit as by more the unsuccessful ands whin the lab impact and the could be impact and the exploit and the lab impact an	ense allow an atacker to for their cute e to a son the athese difying derlying derlying are to a sith root allow to other s.			22101	9/720
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696						H-CIS- 22101	
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote						H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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 & CVI	E ID		Pa	tch	NCII	PC ID
			Malwa RTF a more vulnes sectio	er to by are and l nd RAR informa rabilities n of this	File Poli file type tion abo s, see the advisor	cies for s. For ut these Details y.	e				
			CVE I	D : CVE-	2019-1	2697					
firepower_41	40										
Improper Encoding or Escaping of Output	02-10-2019	7.2	multi- Firepo (FTD) authe escape FTD in comm privile names vulnes insuff under attack vulnes critica filesys could execu privile names the at runnin	ole vulned instance ower The Softwar Inticated, ethe correstance at ands with eges in the space. The could rabilities al files or stem. As allow the te comme eges with space. The could space at acker to the space of the comme eges with the comme eges with space. The could space of the comme eges with the	e feature reat Define could a local at a local at a local at and execution he host he sare due to tection esystem a lexploit is by module attack a local and switchin the local and switching the local and	e of Cisco ense allow an etacker t for their cute e to as on the as on the difying derlying all exploi er to ith root nost d allow other s.	o n co	I/A		H-CIS- 22101	FIRE- 9/723
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root					I/A		H-CIS- 22101	FIRE- 9/724
CV Scoring Scal	e 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
			privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these vulnerabilities by modifying critical files on the underlying filesystem. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running FTD instances. CVE ID: CVE-2019-12675		
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-FIRE- 221019/725
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.	N/A	H-CIS-FIRE- 221019/726

Weakness	Publish Date	cvss	Description & CVE ID					Patch	NCIII	PC ID
			CVE I	D : CVE-	2019-1	2697				
firepower_41	50									
Improper Encoding or Escaping of Output	02-10-2019	7.2	multi- Firepo (FTD) auther escap FTD in common privile name vulne insuff under attack vulne critica filesyst could execu privile name the at runni	ple vulne instance ower The Softwar nticated e the constance nands wite ges in tabilities of the could rabilitie at files of stem. As allow the commeges wite space. The could ge the commeges with the comment of th	e feature reat Def re could , local at antainer f and exec th root he host he se s are duc cotection esystem d exploit s by mod a the un successf ae attack hin the l his could o impact astance	e of Cisco ense allow as stacker to cate or their cute e to ns on the . An these difying derlying ul explo ter to ith root nost d allow t other s.	o n n n n n n n n n n n n n n n n n n n	A	H-CIS- 22101	
Improper Encoding or Escaping of Output	02-10-2019	7.2	Multiple vulnerabilities in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their FTD instance and execute commands with root privileges in the host namespace. These vulnerabilities are due to insufficient protections on the underlying filesystem. An attacker could exploit these					A	H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
			critical filesystem could execu privil name the at runni	rabilities al files on stem. A s allow th te comm eges wit space. T tacker to ng FTD i D: CVE-	n the un successfue attack nands w hin the l his could o impact nstance	derlying ul explo er to ith root nost d allow cother s.	it			
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	ple vulne Firepow are Dete allow and chenticat ker to by are and and RAR informa rabilities on of this	ection Entered File Polition about the advisor	em ngine ote nfigured cies for es. For out these e Details	N/A	1	H-CIS- 22101	
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	ple vulne Firepower are Dete allow are thenticate ker to by are and and RAR informa rabilities on of this	ection Enterection Enterection The sed, reministed pass confile Polition about the second advisor	em ote ofigured cies for es. For out these e Details	N/A	Λ.	H-CIS- 22101	
asa_5500-x										
Improper Input Validation	02-10-2019	5	Cisco Softw	ple vulno Firepow are Dete allow ar	ver Syste ection E	em	N/A	1	H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
			attack Malw RTF a more vulne sectio	thenticate to by are and RAR informa rabilities n of this D: CVE-	pass cor File Poli file type tion abo s, see the advisor	nfigured cies for es. For out these e Details				
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	ple vulne Firepow are Dete allow ar chenticat are and in are and in informa rabilities n of this	ection Er ection Er ed, rem pass cor File Poli file type tion abo s, see the advisor	em ngine ote nfigured cies for es. For out these e Details	N/A	A	H-CIS- 22101	_
firepower_10	10									
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	ple vulne Firepow are Dete allow ar chenticat ter to by are and I nd RAR informa rabilities n of this	ver Systements of the control of the	N/A	A	H-CIS- 22101		
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut	ple vulne Firepow are Dete allow ar henticat	ver Syste ection Er n ced, rem	em ngine ote	N/A	A	H-CIS- 22101	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6					7-8	8-9	9-10

Weakness	Publish Date	cvss		Descript	ion & CV	E ID	Р	atch	NCII	PC ID
			RTF a more vulne section	are and and RAR informa rabilities on of this D : CVE-	file type tion abo s, see the advisor	es. For out these e Details ry.				
firepower_11	20		CVEI	D.CVE-	2019-1	2097				
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne	ple vulne Firepow rare Dete allow and thenticat ker to by are and and RAR informa rabilities	rer Syste ection Er ed, rem pass cor File Poli file type tion abo	em ngine ote nfigured cies for es. For out these e Details			H-CIS- 22101	
			CVE I	D : CVE-	2019-1	2696				
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697					H-CIS- 22101	FIRE- 9/736
firepower_11	40						1		1	
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for				N/A		H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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		Patch	NCIII	PC ID
			more vulne	nd RAR informa rabilities n of this	tion abo					
			CVE I	D : CVE-	2019-1	2696				
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697					A	H-CIS- 22101	
financy 21	10		CVE I	D : CVE-	2019-1					
firepower_21	10		1				ı		1	
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malw RTF a more vulne sectio	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696				A	H-CIS- 22101	
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these					A	H-CIS- 22101	
CV Scoring Scal (CVSS)	e 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		Descript	on & CV	E ID	Р	atch	NCII	PC ID
				rabilities n of this		e Details				
				n or uns D : CVE-						
finanayyan 21	20		CVEI	D:CVE-	2019-1	2097				
firepower_21	.20		Maaleia	-ll	نعنانوا ومد					
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malwa RTF a more vulnes	Firepoware Determenticater to by are and RAR informarabilities n of this	rer Syste ction En ed, rem pass con File Poli file type tion abo s, see the advison	ote ofigured cies for es. For out these e Details			H-CIS- 22101	
			CVE I	D : CVE-	2019-1	2696				
Improper Input Validation	02-10-2019	5	Cisco Softw could unaut attack Malwa RTF a more vulnes	Firepoware Deterallow ar henticater to by are and Ind RAR informa	rer Syste ction En ed, rem pass con File Poli file type tion abo s, see the advison	ote ofigured cies for es. For out these e Details			H-CIS- 22101	
firepower_21	30								l	
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details						H-CIS- 22101	
CV Scoring Scal (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
			section of this advisory.		
			CVE ID : CVE-2019-12696		
Improper Input Validation	Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.		N/A	H-CIS-FIRE- 221019/744	
			CVE ID : CVE-2019-12697		
firepower_21	40				
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-FIRE- 221019/745
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.	N/A	H-CIS-FIRE- 221019/746

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-12697		
firepower_70	00			1	
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-FIRE- 221019/747
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	H-CIS-FIRE- 221019/748
firepower_80	00				
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory.	N/A	H-CIS-FIRE- 221019/749

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-12696		
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	H-CIS-FIRE- 221019/750
firepower_th	reat_defense_	for_isr			
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-FIRE- 221019/751
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	H-CIS-FIRE- 221019/752

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
ftd_virtual					
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-FTD 221019/753
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	H-CIS-FTD 221019/754
isa_3000					
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-ISA 221019/755

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	H-CIS-ISA 221019/756
ngipsv_for_vn	nware				
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12696	N/A	H-CIS-NGIP- 221019/757
Improper Input Validation	02-10-2019	5	Multiple vulnerabilities in the Cisco Firepower System Software Detection Engine could allow an unauthenticated, remote attacker to bypass configured Malware and File Policies for RTF and RAR file types. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID: CVE-2019-12697	N/A	H-CIS-NGIP- 221019/758
firepower_10	00				

Weakness	Publish Date	CVSS		Descripti	on & CVI	E ID		Patch	NCII	PC ID
Improper Input Validation	02-10-2019	7.2	CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges. CVE ID: CVE-2019-12699 A vulnerability in the configuration of the Pluggable Authentication Module (PAM)					'A	H-CIS- 22101	FIRE- 9/759
Uncontrolled Resource Consumption	02-10-2019	6.8	config Auther used in Threat Softw Manay Softw auther to cau (DoS) vulner impro- manay user stattack vulner an affin perfor	guration	of the Pin Modul Firepow e (FTD) o Firepo Center (Cisco Find allow a remote ial of se on. The s due to ource in the con anagen exploit by connected any	e (PAM) er ower FMC) KOS an e attacke rvice ontext of nent. An this ecting to	r N/	'A	H-CIS- 22101	FIRE- 9/760
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Dat	e CVSS		Descript	ion & CV	E ID	ı	Patch	NCIII	PC ID
			succe the at resou to rel condi vulne needs the sy	Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system. CVE ID: CVE-2019-12700						
firepower_21	00									
Improper Input Validation	02-10-201	9 7.2	CLI of and C Defendation allow attack on the system privil vulne insuff An attack crafted explodattack on the on the control o	Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges.					H-CIS- 22101	
Uncontrolled Resource Consumption	02-10-201	9 6.8	config Author used: Threat Softwo Manat Softwo	nerabilit guration enticatio in Cisco nt Defens rare, Cisco gement rare, and rare coul	of the P n Modul Firepow se (FTD) so Firepo Center (Cisco F	e (PAM) er ower FMC) KOS			H-CIS-FIRE- 221019/762	
CV Scoring Scal (CVSS)	e 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
			authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper resource management in the context of user session management. An attacker could exploit this vulnerability by connecting to an affected system and performing many simultaneous successful Secure Shell (SSH) logins. A successful exploit could allow the attacker to exhaust system resources and cause the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker needs valid user credentials on the system. CVE ID: CVE-2019-12700		
firepower_41	00				
Improper Input Validation	02-10-2019	7.2	Multiple vulnerabilities in the CLI of Cisco FXOS Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute commands on the underlying operating system (OS) with root privileges. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by including crafted arguments to specific CLI commands. A successful exploit could allow the attacker to execute commands	N/A	H-CIS-FIRE- 221019/763

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss		Descript	ion & CV	E ID	F	atch	NCII	PC ID
			on the underlying OS with root privileges. CVE ID: CVE-2019-12699							
			CVE I	D : CVE-	2019-1	2699				
ic3000_indus	trial_compute	_gatev	vay							
Uncontrolled Resource Consumption	02-10-2019	4	based of Cisc Compan aurattack service affect vulne the affingred exploopenismul web-kinterf A succeallow DoS cobased preventions.	thentica xer to ca ce (DoS) ed device rability of fected so operly mander rces. And it this vurant it this vurant and a large taneous oased mander	ement in 200 Industry conditions and december and decembe	nterface strial uld allow note mial of on on an ecause system r could lity by ner of s on the ent d device ould cause a web- nterface, ons.	N/A		H-CIS- 22101	-IC30- 19/764
asa_5540									_	
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in				N/A		H-CIS- 22101	-ASA 19/765
CV Scoring Scal	e 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
			a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256		
asa_5545-x					
Uncontrolled Resource Consumption	02-10-2019	7.8	A vulnerability in the Internet Key Exchange version 1 (IKEv1) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper management of system memory. An attacker could exploit this vulnerability by sending malicious IKEv1 traffic to an affected device. The attacker does not need valid credentials to	N/A	H-CIS-ASA 221019/766

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			authenticate the VPN session, nor does the attacker's source address need to match a peer statement in the crypto map applied to the ingress interface of the affected device. An exploit could allow the attacker to exhaust system memory resources, leading to a reload of an affected device. CVE ID: CVE-2019-15256		
compal			0.2.2.0.002.2019.2020		
ch7465lg					
Improper Input Validation	02-10-2019	7.5	Compal CH7465LG CH7465LG-NCIP-6.12.18.24-5p8-NOSH devices have Incorrect Access Control because of Improper Input Validation. The attacker can send a maliciously modified POST (HTTP) request containing shell commands, which will be executed on the device, to an backend API endpoint of the cable modem. CVE ID: CVE-2019-13025	N/A	H-COM- CH74- 221019/767
fiberhome					
hg2201t					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-10-2019	5	/var/WEB-GUI/cgi-bin/downloadfile.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows preauthentication Directory Traversal for reading arbitrary files. CVE ID: CVE-2019-17187	N/A	H-FIB-HG22- 221019/768
FON					

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	1-2	2-3	5	7	3-0	0-7	7-8	0-3	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fon2601e-se					
Improper Input Validation	04-10-2019	7.8	FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities. CVE ID: CVE-2019-6015	N/A	H-FON- FON2- 221019/769
fon2601e-re					
Improper Input Validation	04-10-2019	7.8	FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities. CVE ID: CVE-2019-6015	N/A	H-FON- FON2- 221019/770
fon2601e-fsw	V-S				
Improper Input Validation	04-10-2019	7.8	FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.	N/A	H-FON- FON2- 221019/771

Weakness	Pu	blish Date	cvss		Descript	ion & CV	E ID	F	Patch	NCIII	PC ID	
				CVE I	D : CVE-	2019-6	015					
fon2601e-fsw	/-b											
Improper Input Validation	04-	-10-2019	7.8	FON2 FON2 firmw earlie they r resolv is exp be lev ampli other	ON2601E-SE, FON2601E-RE, ON2601E-FSW-S, and ON2601E-FSW-B with rmware versions 1.1.7 and arlier contain an issue where ey may behave as open solvers. If this vulnerability exploited, FON routers may eleveraged for DNS applification attacks to some ther entities. VE ID: CVE-2019-6015		e N/A		H-FON FON2- 22101			
govicture	l											
pc530												
Missing Authenticati on for Critical Function	01-	-10-2019	10	unaut acces	Victure PC530 devices allow unauthenticated TELNET access as root. CVE ID: CVE-2019-15940		N/A		H-GOV PC53- 22101			
socomec				•								
diris_a-40												
Insufficiently Protected Credentials	09-	-10-2019	10	web i DIRIS 48250 attack device URI.			web interface on socomec DIRIS A-40 devices before 48250501 allows a remote attacker to get full access to a device via the /password.jsn		N/A		H-SOC 22101	
vzug												
combi-stream	n_ms	slq										
Improper Authenticati on	06-	-10-2019	5	Zug C	An issue was discovered on V- Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There			SLQ net R07		H-VZU- COMB- 221019/775		
CV Scoring Scal (CVSS)	е	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 & CVI	E ID		Patch	NCII	PC ID			
			(e.g., l attack brute	orutefore ockout) xer migh force the nticate o	establis t be able passwo	hed. An e to ord to							
1			CVE I	D : CVE-	2019-1	7215							
Improper Authenticati on	06-10-2019	7.5	An issue was discovered on V- Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. Password authentication uses MD5 to hash passwords. Cracking is possible with minimal effort. CVE ID: CVE-2019-17216			H-VZU COMB 22101							
Cross-Site Request Forgery (CSRF)	06-10-2019	6.8	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no CSRF protection established on the web service. CVE ID: CVE-2019-17217				N/A	L	H-VZU COMB 22101				
Missing Encryption of Sensitive Data	06-10-2019	5	Zug C device and b defau the w via ht interc comm service	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the communication to the web service is unencrypted via http. An attacker is able to intercept and sniff communication to the web service.		Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the communication to the web service is unencrypted via http. An attacker is able to intercept and sniff communication to the web service.		ig Combi-Steam MSLQ evices before Ethernet R07 d before WLAN R05. By fault, the communication to e web service is unencrypted a http. An attacker is able to tercept and sniff mmunication to the web			1	H-VZU COMB 22101	
Improper Authenticati on	06-10-2019	5.8	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the device does not enforce any authentication. An				N/A	N/A		- - 9/779			
CV Scoring Scal (CVSS)	e 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	NCIIF	C ID		
			adjacent attacker is able to use the network interface without proper access control.								
			CVE ID : CVE-2019-17219								
Xerox											
atlalink_b8045											
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184			/	.	H-XER- ATLA- 221019/780			
atlalink_b8055											
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184				/	1	H-XER- ATLA- 221019/781		
atlalink_b8065											
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184				/		H-XER- ATLA- 221019/782		
atlalink_b8075											
Improper	04-10-2019	7.5	Xerox AtlaLink			N/A	1	H-XER-			
CV Scoring Scal (CVSS)	e 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			Pa	tch	NCIII	PC ID		
Privilege Management			B8045/B8055/B8065/B8075/B8090 C8030/C8035/C8045/C8055/C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184			/			ATLA- 221019/783		
atlalink_b809	0										
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184				/	N/A		H-XER- ATLA- 221019/784	
atlalink_c803	0										
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184				/	N/A		H-XER- ATLA- 221019/785	
atlalink_c8035											
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184			/	N/A		H-XER- ATLA- 221019/786		
CV Scoring Scal (CVSS)	e 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				
atlalink_c8045									
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184	N/A	H-XER- ATLA- 221019/787				
atlalink_c8055									
Improper Privilege Management	04-10-2019	7.5	Xerox AtlaLink B8045/B8055/B8065/B8075/ B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184	N/A	H-XER- ATLA- 221019/788				
atlalink_c807	atlalink_c8070								
Improper Privilege Management	Xerox AtlaLink B8045/B8055/B8065/B8075 B8090 C8030/C8035/C8045/C8055/ C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges. CVE ID: CVE-2019-17184		N/A	H-XER- ATLA- 221019/789					