

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

16 - 31 Oct 2019

Vol. 06 No. 20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Application			
Adobe						
experience_r	nanager					
Improper Restriction of XML External Entity Reference ('XXE')	25-10-2019	5	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8086	https://helpx. adobe.com/se curity/produc ts/experience - manager/aps b19-48.html	A-ADO-EXPE- 041119/1	
Improper Restriction of XML External Entity Reference ('XXE')	25-10-2019	5	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8087	https://helpx. adobe.com/se curity/produc ts/experience - manager/aps b19-48.html	A-ADO-EXPE- 041119/2	
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component ('Injection')	25-10-2019	7.5	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8088	https://helpx. adobe.com/se curity/produc ts/experience - manager/aps b19-48.html	A-ADO-EXPE- 041119/3	
Improper Neutralizati on of Input	24-10-2019	4.3	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a reflected	https://helpx. adobe.com/se curity/produc	041119/4	
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Puk	olish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')				vulne explo sensit disclo	site scri rability. itation c tive info osure. D : CVE -	Success ould lea rmation	d to	ts/exper - manager b19-48.l	·/aps		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-2	10-2019	4.3	Mana 6.2, 6 store vulne explo sensit disclo	6.2, 6.1, and 6.0 have a stored cross site scripting vulnerability. Successful exploitation could lead to sensitive information				helpx. om/se roduc rience r/aps ntml	A-ADO- 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-1	10-2019	4.3	Mana 6.3 ha script Succe could escala	Adobe Experience Manager versions 6.4 and 6.3 have a stored cross site scripting vulnerability. Successful exploitation could lead to privilege escalation. CVE ID: CVE-2019-8080				helpx. om/se roduc rience -/aps ntml	A-ADO- 041119	
Improper Authenticati on	25-2	10-2019	5	Mana 6.3 ar authe vulne explo sensit disclo	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have an authentication bypass vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8081				helpx. om/se roduc rience r/aps ntml	A-ADO- 041119	
Improper Restriction of XML External Entity Reference	25-1	10-2019	5	Mana and 6 exter vulne explo	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information			https://adobe.co curity/p ts/exper - manager	om/se roduc rience	A-ADO- 041119	
CV Scoring Sca (CVSS)	ile	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
('XXE')			disclosure.	b19-48.html	
			CVE ID : CVE-2019-8082		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	25-10-2019	4.3	Adobe Experience Manager versions 6.5, 6.4 and 6.3 have a cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8083	https://helpx. adobe.com/se curity/produc ts/experience - manager/aps b19-48.html	A-ADO-EXPE- 041119/9
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	25-10-2019	4.3	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8084	https://helpx. adobe.com/se curity/produc ts/experience - manager/aps b19-48.html	A-ADO-EXPE- 041119/10
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	25-10-2019	4.3	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8085	https://helpx. adobe.com/se curity/produc ts/experience - manager/aps b19-48.html	A-ADO-EXPE- 041119/11
Cross-Site Request Forgery (CSRF)	25-10-2019	4.3	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a cross-site request forgery vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8234	https://helpx. adobe.com/se curity/produc ts/experience - manager/aps b19-48.html	A-ADO-EXPE- 041119/12
download_m	anager				
CV Scoring Sca	ole 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	3	7-8	

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
Incorrect Permission Assignment for Critical Resource	17-10-2019	7.5	version insection vulne exploon privil	e Downlons 2.0.0 ure file perability. itation cege esca	.363 ha ermissi Success ould lea lation.	ve an ons ful d to	https://adobe.co curity/p ts/adm/ 19-51.ht	om/se roduc apsb	A-ADO- DOWN- 041119	
acrobat_dc										
Out-of- bounds Read	17-10-2019	4.3	version and e 2017, earlie and e 2015, earlie bound Succe could disclo	e Acroba ons , 201 arlier, .011.301 er, 2017.0 arlier, .006.305 er, and .006.305 er have a ds read v essful exp lead to i osure . D: CVE-	9.012.2 48 and 011.301 03 and n out-of vulneration	0040 48 Septility.	https://adobe.co curity/p ts/acrob sb19-49	om/se roduc oat/ap	A-ADO- 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a cross-site scripting vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8160				https://adobe.co curity/p ts/acrob sb19-49	om/se roduc oat/ap	A-ADO- 041119	
Incorrect	17-10-2019	7.5	Adobe Acrobat and Reader			https://	helpx.	A-ADO-	ACRO-	
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
Type Conversion or Cast			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8161	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/16
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a race condition vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8162	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/17
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/18
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				Pato	h	NCIIP	C ID
			could disclo	ssful explead to be sure. D: CVE-	informa	tion				
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8164				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Write	17-10-2019	6.8	version and explored and explor	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.				nelpx. om/se roduc at/ap .html	A-ADO- 041119	
Improper Restriction of Operations within the	17-10-2019	6.8	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148				https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		A-ADO-ACRO- 041119/21	
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
Bounds of a Memory Buffer			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a buffer overrun vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8166		
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8167	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/22
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/23

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	P	atch	NCIIF	PC ID
			CVE I	D : CVE-	2019-8	168				
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8169				adobe curity ts/acr	//helpx. .com/se /produc obat/ap 49.html	A-ADO- 041119	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.				adobe curity ts/acr	//helpx. .com/se /produc obat/ap 49.html	A-ADO- 041119	
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and				adobe curity ts/acr	//helpx. .com/se /produc obat/ap 49.html	A-ADO- 041119	
CV Scoring Sca (CVSS)	lle 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				Pato	h	NCIIP	CID
			earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8171							
Out-of- bounds Read	17-10-2019	4.3	version and e 2017 earlie 2015 earlie bound Succession disclared	e Acroba ons , 201 arlier, .011.301 er, 2017. arlier, .006.305 er, and .006.305 er have a ds read v essful exp lead to osure .	9.012.2 .48 and 011.301 .03 and n out-of vulneral oloitatio	on tion	https://l adobe.co curity/p ts/acrob sb19-49	m/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Read	17-10-2019	4.3	version and e 2017 earlie 2015 earlie bound Succession disclared	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8173			https://l adobe.co curity/p ts/acrob sb19-49	m/se roduc at/ap	A-ADO 041119	
NULL Pointer Dereference	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,				https://l adobe.co curity/p	m/se	A-ADO- 041119	
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				Pato	h	NCIIP	CID
			earlie and e 2015 earlie 2015 earlie point vulne explo arbiti	er, 2017. arlier, .006.305 er, and .006.305 er have a er dereferability. itation c cary code	011.301 603 and n untrus erence Success ould lea	sted ful d to ion .	ts/acrob sb19-49			
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.				https://badobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Use After Free	17-10-2019	6.8	version and example and example and example 2015 example free versions.	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary				helpx. om/se roduc at/ap .html	A-ADO- 041119	
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
			code execution .		
			CVE ID : CVE-2019-8176		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/32
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8178	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/33
Use After Free	versions , 2019.0 and earlier, 2017.011.30148 earlier, 2017.011 and earlier,		2017.011.30148 and earlier, 2017.011.30148	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/34

3-4

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Pu	blish Date	CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIF	PC ID
				earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8179							
Use After Free	17-	10-2019	6.8	version and example and example and example arrive free versions of the could code	ons, 201 earlier, .011.303 er, 2017. earlier, .006.305 er, and .006.305 er have a vulnerab essful ex l lead to execution	.011.301 503 and 503 and in use af ility. ploitatio arbitrar	0040 48 ter on	https://adobe.c curity/pts/acrolsb19-49	om/se oroduc bat/ap	A-ADO- 041119	
Use After Free	17-	10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8181			https://adobe.c curity/p ts/acrol sb19-49	om/se oroduc bat/ap	A-ADO- 041119		
Out-of-	17-	10-2019	5	Adobe Acrobat and Reader			eader	https://	helpx.	A-ADO-	ACRO-
CV Scoring Sca (CVSS)	ale	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
bounds Read			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8182	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/37
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	9.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8183	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/38
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/39
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				Pato	h	NCIIP	C ID
			Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8184							
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8185				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Write	17-10-2019	10	version and e 2017. earlie and e 2015. earlie bound vulne explo	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .				nelpx. om/se roduc at/ap .html	A-ADO- 041119	
Use After Free	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148				https://b adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
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
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8187		
Use After Free	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8188	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/43
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/44

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	C ID	
			CVE I	D : CVE-	2019-8	189				
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8190				https://adobe.co curity/pts/acrob sb19-49	om/se oroduc oat/ap	A-ADO- 041119	
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.				https://adobe.co curity/pts/acrob sb19-49	om/se oroduc oat/ap	A-ADO- 041119	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and				https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		A-ADO- 041119	
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	Pul	blish Date	e CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIF	PC ID
				free v Succe could code	earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8192						
Out-of- bounds Read	17-	10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8193				https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Read	17-	10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8194			https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		A-ADO- 041119		
NULL Pointer Dereference	17-	10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,				https://ladobe.co	m/se	A-ADO- 041119	
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-3 3-4 4-5 5-6		5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID				Pato	h	NCIIP	CID
			earlie and e 2015. earlie 2015. earlie point vulne explo arbitr	o11.301 or, 2017. arlier, o06.305 or, and o06.305 or have a er dereforability. itation contacts ary code D: CVE-	011.301 603 and n untrus erence Success ould lea	sted ful d to ion .	ts/acrob sb19-49			
NULL Pointer Dereference	17-10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution.				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary			https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		A-ADO- 041119		
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
			code execution .		
			CVE ID : CVE-2019-8197		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/53
Out-of- bounds Write	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/54
Incorrect Type Conversion or Cast	versions, 2019.012.20 and earlier, 2017.011.30148 and earl		2017.011.30148 and earlier, 2017.011.30148 and earlier,	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/55

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8200		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8201	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/56
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8202	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/57
Use After	17-10-2019	6.8	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-
CV Scoring Sci (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pul	blish Date	e CVSS	Description & CVE ID				Pato	:h	NCIIP	CID
Free				versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8203				adobe.co curity/p ts/acrob sb19-49	roduc at/ap	041119	/58
Out-of- bounds Read	17-	10-2019	6.8	version and e 2017 earlie 2015 earlie bound Succession disclared	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.				helpx. om/se roduc oat/ap .html	A-ADO- 041119	
NULL Pointer Dereference	17-	10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference			https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		A-ADO- 041119		
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	Pul	blish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
				explo	rability. itation c rary code	ould lea	d to				
				CVE I	D : CVE	·2019-8	205				
Out-of- bounds Write	17-	10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8206				https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Read	17-	10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8207				https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Use After Free	17-	10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148				https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		A-ADO- 041119	
CV Scoring Scal (CVSS)	le	0-1	1-2	2-3	2-3 3-4 4-5 5-6		5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8208		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8209	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/64
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/65

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	C ID	
			CVE I	D : CVE-	2019-8	210				
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8211				https://adobe.c curity/j ts/acro sb19-49	om/se produc bat/ap	A-ADO- 041119	
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.				https://adobe.cocurity/jts/acrosb19-49	om/se produc bat/ap	A-ADO- 041119	
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and				https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		A-ADO- 041119	
CV Scoring Sca (CVSS)	lle 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			Pato	:h	NCIIP	CID
				free v Succe could code	earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8213						
Use After Free	17-	10-2019	7.5	Adob versi and e 2017 earlie and e 2015 earlie free v Succe could code	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.			https://adobe.co curity/p ts/acrob sb19-49	om/se roduc oat/ap	A-ADO- 041119	
Use After Free	17-	10-2019	7.5	versi and e 2017 earlie and e 2015 earlie free v Succe could code	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.			https://adobe.co curity/p ts/acrob sb19-49	om/se roduc oat/ap	A-ADO-ACRO- 041119/70	
Out-of- bounds Read	17-	10-2019	5	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier,			https://adobe.co	m/se	A-ADO- 041119		
CV Scoring Sc (CVSS)	ale	0-1	1-2	1-2 2-3 3-4 4-5 5-6		5-6	6-7	7-8	8-9	9-10	

Weakness	Publish	Date	cvss	Description & CVE ID			Pato	h	NCIIP	C ID	
				2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8216				ts/acrob sb19-49			
Use After Free	17-10-	2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.			https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119		
Out-of- bounds Read	17-10-2	2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information			https://badobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119		
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
			disclosure.		
			CVE ID : CVE-2019-8218		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/74
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8220	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/75
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/76

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Pul	blish Date	cvss	D	Description & CVE ID			Pat	ch	NCIIF	PC ID
				2015 earlie free v Succe could code	vulnerab essful ex l lead to execution	n use af ility. ploitatio arbitrar on .	n y				
Out-of- bounds Read	17-	10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			https://adobe.c curity/ ts/acro sb19-4	om/se produc bat/ap	A-ADO- 041119		
Use After Free	17-	10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8223			https://adobe.c curity/ ts/acro sb19-4	om/se produc bat/ap	A-ADO- 041119		
Use After	17-	10-2019	6.8	Adobe Acrobat and Reader			https://	/helpx.	A-ADO-	ACRO-	
CV Scoring Sca (CVSS)	ale	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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
Free				versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8224				adobe.co curity/p ts/acrob sb19-49	roduc at/ap	041119	/79
Use After Free	17-	10-2019	6.8	version and e 2017 earlie 2015 earlie free version could	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.			https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO-, 041119	
Information Exposure	17-	10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an incomplete implementation of			https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO 041119		
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				Pato	h	NCIIP	C ID
			security mechanism vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8226							
Inadequate Encryption Strength	23-10-2019	10	Adoboversion and e 2019 earlie 2017 earlie 2015 earlie 2015 earlie Insuff Encry Succession could feature content user.	e Acroba ons 2019 arlier; .012.200 or version .011.301 or version .006.304 or version .006.304 or version .tr vers	at and Re 9.012.20 935 and ns; 42 and ns; 43 and ns; 497 and ns have Robust alnerabilistic Security s in the	eader 034 an lity. n	N/A		A-ADO- 041119	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier; 2019.010.20099 and earlier versions; 2017.011.30140 and earlier version; 2017.011.30138 and earlier version; 2015.006.30495 and earlier versions; 2015.006.30493 and earlier versions have a Path Traversal				N/A		A-ADO- 041119	
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
			vulnerability. Successf exploitation could lead Information Disclosure the context of the curr user. CVE ID: CVE-2019-82	l to e in ent		
acrobat_read	ler_dc					
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reversions, 2019.012.20 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerable Successful exploitation could lead to informat disclosure.	http add cur ts/a sb1 ility.	ps://helpx. bbe.com/se rity/produc acrobat/ap .9-49.html	A-ADO-ACRO- 041119/84
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	4.3	Adobe Acrobat and Reversions, 2019.012.20 and earlier, 2017.011.30148 and earlier, 2017.011.3014 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a cross-sit scripting vulnerability Successful exploitation could lead to informat disclosure. CVE ID: CVE-2019-81	http add cur ts/a sb1	ps://helpx. bbe.com/se rity/produc acrobat/ap .9-49.html	A-ADO-ACRO- 041119/85
Incorrect Type	17-10-2019	7.5	Adobe Acrobat and Reversions, 2019.012.20		ps://helpx. obe.com/se	A-ADO-ACRO- 041119/86
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			Pato	h	NCIIP	C ID	
Conversion or Cast			and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8161				curity/p ts/acrob sb19-49	at/ap		
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	17-10-2019	6.8	version and e 2017 earlie 2015 earlie conditions could code	e Acroba ons, 201 arlier, .011.301 er, 2017. arlier, .006.305 er, and .006.305 er have a ction vulue essful exp lead to a executio	9.012.2 48 and 011.301 603 and race nerability coloritation arbitrary	0040 48 y. n	https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119		
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
			could lead to information disclosure . CVE ID : CVE-2019-8163		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8164	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/89
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8165	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/90
Improper Restriction of Operations within the Bounds of a	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier,	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/91

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			2015.006.30503 and earlier, and 2015.006.30503 and earlier have a buffer overrun vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8166		
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8167	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/92
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8168	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/93

Weakness	Publish Date	cvss	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
Incorrect Type Conversion or Cast	17-10-2019	7.5	versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8169				https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO 041119	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	6.8	version and e 2017, earlie 2015, earlie overf. Succe could code	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.				helpx. om/se roduc at/ap .html	A-ADO-, 041119	
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-			https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO-, 041119		
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	NCIIPC ID
			bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8171		
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8172	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/97
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8173	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/98
NULL Pointer Dereference	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap	A-ADO-ACRO- 041119/99

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8174	sb19-49.html	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/100
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/101
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				Pate	ch	NCIIP	C ID
			CVE I	D : CVE	-2019-8	176				
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8177				https://adobe.co curity/p ts/acrob sb19-49	om/se oroduc oat/ap	A-ADO- 041119	
Use After Free	17-10-2019	6.8	version and e 2017 earlie 2015 earlie free version could	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.				helpx. om/se oroduc oat/ap o.html	A-ADO- 041119	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and				https://adobe.co curity/p ts/acrob sb19-49	om/se oroduc oat/ap	A-ADO- 041119	
CV Scoring Sca (CVSS)	o-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Puk	olish Date	CVSS	D	Description & CVE ID			Pato	h	NCIIF	PC ID
				free v Succe could code	earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8179						
Use After Free	17-2	10-2019	6.8	version and example 2017 earlies 2015 earlies free versions could code	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8180			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Use After Free	17-1	10-2019	6.8	version and example and example and example arrive free version code	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8181			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Read	17-2	10-2019	5	versi	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,			https://kadobe.co	m/se	A-ADO- 041119	
CV Scoring Sca (CVSS)	ale	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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
				earlie and e 2015 earlie 2015 earlie boun Succe could disclo	.011.301 er, 2017. er, 2017. arlier, .006.305 er, and .006.305 er have a ds read v essful exp l lead to osure.	011.301 03 and 03 and n out-of vulneral oloitatio informa	oility. n tion	ts/acrob sb19-49			
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-1	.0-2019	9.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8183				https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Read	17-1	.0-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information				https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
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
			disclosure.		
			CVE ID : CVE-2019-8184		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/110
Out-of- bounds Write	17-10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8186	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/111
Use After Free	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/112

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8187		
Use After Free	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/113
			Successful exploitation could lead to arbitrary code execution . CVE ID : CVE-2019-8188 Adobe Acrobat and Reader		
Out-of- bounds Read	17-10-2019	4.3	versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8189	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/114
Out-of-	17-10-2019	4.3	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-
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	NCIIPC ID
bounds Read			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8190	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/115
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/116
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/117
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	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
			could code	essful explead to a lead t	arbitrary n .	у				
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8193				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
Out-of- bounds Read	17-10-2019	5	version and e 2017, earlie 2015, earlie bound Succe could	2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
NULL Pointer Dereference	17-10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148				https://b adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
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
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8195		
NULL Pointer Dereference	17-10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/121
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-819	7	
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Read versions, 2019.012.2004 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/123
Out-of-	17 10 2010	7.5	Adobe Acrobat and Read versions, 2019.012.2004 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and	https://helpx.adobe.com/se	A-ADO-ACRO-
bounds Write	17-10-2019	7.5	2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead trarbitrary code execution CVE ID: CVE-2019-819	0	041119/124
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Read versions, 2019.012.2004 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and	https://helpx. adobe.com/se	A-ADO-ACRO- 041119/125
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	NCIIPC ID
			earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8200		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8201	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/126
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8202	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/127
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,	https://helpx. adobe.com/se curity/produc	A-ADO-ACRO- 041119/128

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish	Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				earlie and e 2015 earlie free v Succe could code	on 11.301 or, 2017. arlier, on 6.305 or, and on 6.305 or have a rulnerab essful exp lead to executio D: CVE-	011.301 603 and 603 and n use affility. ploitatio arbitrary	ter n y	ts/acrob			
Out-of- bounds Read	17-10-2	2019	6.8	version and e 2017 earlie 2015 earlie bound Succession disclared	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.				helpx. om/se roduc at/ap .html	A-ADO- 041119	
NULL Pointer Dereference	17-10-2	2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to				https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
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
			arbitrary code execution .		
			CVE ID : CVE-2019-8205		
Out-of- bounds Write	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/131
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8207	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/132
Use After Free	17-10-2019 6.8		Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/133

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Pu	blish Date	cvss		escriptio	n & CVE I	D	Pat	ch	NCIIF	PC ID
				2015 earlie free v Succe could code	vulnerab essful ex l lead to execution	n use af oility. ploitatio arbitrar	n y				
Use After Free	17-	10-2019	6.8	version and example and example and example arrive free version code	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8209 Adobe Acrobat and Reader				/helpx. om/se produc bat/ap 9.html	A-ADO- 041119	
Use After Free	17-	10-2019	6.8	code execution . CVE ID : CVE-2019-8209			https://adobe.c curity/j ts/acro sb19-49	om/se produc bat/ap	A-ADO- 041119		
Use After	17-	10-2019	7.5	Adob	e Acrob	Acrobat and Reader		https://	/helpx.	A-ADO-	ACRO-
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Puk	olish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
Free				and e 2017 earlie and e 2015 earlie free v Succe could code	arlier, .011.301 er, 2017. arlier, .006.305 er, and .006.305 er have a vulnerab essful exition	011.301 503 and 503 and in use af ility. ploitatio arbitrar	48 ter n y	adobe.co curity/p ts/acrob sb19-49	roduc oat/ap	041119	/136
Use After Free	17-	10-2019	7.5	version and experience	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.				helpx. om/se oroduc oat/ap .html	A-ADO- 041119	
Use After Free	17-	10-2019	7.5	version and e 2017 earlie 2015 earlie 2015 earlie	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability.				helpx. om/se oroduc oat/ap .html	A-ADO- 041119	
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	Pul	blish Date	CVSS	C	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
				could	essful explessful expless execution	arbitrar					
				CVE 1	D : CVE	· 2019- 8	3213				
Use After Free	17-	10-2019	7.5	version and example and example and example arrive	e Acroba ons , 201 earlier, .011.301 er, 2017. earlier, .006.305 er, and .006.305 er have a vulnerab essful exp	9.012.2 48 and 011.301 603 and n use af ility. ploitatic arbitrar	.48 Eter	https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
				CVE	D : CVE	2019-8	3214				
Use After Free	17-	10-2019	7.5	version and example and example and example arrive	CVE ID: CVE-2019-8214 Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8215				helpx. om/se roduc at/ap .html	A-ADO- 041119	
Out-of- bounds Read	17-	10-2019	5	version and e	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148			https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
CV Scoring Sca (CVSS)	ıle	0-1	1-2	2-3	3-4	4-5	4-5 5-6 6-7		7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of- bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8216		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8217	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/142
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/143

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	C ID				
			CVE I	D : CVE	-2019-8	218								
Use After Free	17-10-2019	6.8	and e 2017 earlie and e 2015 earlie free v Succe could code	versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8219 Adobe Acrobat and Reader versions, 2019.012.20040				and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .			https://adobe.cc curity/p ts/acrob sb19-49	om/se oroduc oat/ap	A-ADO- 041119	
Use After Free	17-10-2019	7.5	version and experience of the control of the contro	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .				helpx. om/se oroduc oat/ap .html	A-ADO- 041119					
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and				https://adobe.co curity/p ts/acrob sb19-49	om/se oroduc oat/ap	A-ADO- 041119					
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3				6-7	7-8	8-9	9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8221		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8222	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/147
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8223	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	A-ADO-ACRO- 041119/148
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,	https://helpx. adobe.com/se curity/produc	A-ADO-ACRO- 041119/149

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
			earlie and e 2015. earlie free v Succe could	on on one of the color of the c	011.301 003 and 003 and n use affility. oloitatio arbitrary	ter n	ts/acrob sb19-49			
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO 041119	
Information Exposure	17-10-2019	5	code execution . CVE ID: CVE-2019-8225 Adobe Acrobat and Reader versions , 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an incomplete implementation of security mechanism vulnerability. Successful				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	A-ADO- 041119	
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	Pul	blish Date	e (cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIF	PC ID
					infori	nation d	ould lea lisclosur -2019-8	e.				
Inadequate Encryption Strength	23-	10-2019	9 1	10	version and e 2019 earlie 2017 earlie 2015 earlie 2015 earlie 2015 carlie Insuff Encry Succession could feature contents user.	ons 2019 arlier; .012.200 or versio .011.301 or versio .001.304 or versio .006.304 or versio .006.304 or versio ficiently reption versio lead to re bypas ext of the	ns; 42 and ns; 43 and ns; 497 and ns; 498 and Robust ulnerabil ploitatio Security s in the	an lity.	N/A		A-ADO- 041119	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-	10-2019	9 5	5	version and e 2019 earlie 2017 earlie 2015 earlie 2015 earlie Path	Successful exploitation could lead to Security feature bypass in the context of the current user. CVE ID: CVE-2019-8237 Adobe Acrobat and Reader versions 2019.010.20100 and earlier; 2019.010.20099 and earlier versions; 2017.011.30140 and earlier version; 2017.011.30138 and earlier version; 2015.006.30495 and earlier versions; 2015.006.30493 and earlier versions have a Path Traversal vulnerability. Successful			N/A		A-ADO- 041119	
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
			Information Disclosure in the context of the current user. CVE ID: CVE-2019-8238		
creative_clou	ıd				
Improper Privilege Managemen t	23-10-2019	7.5	Creative Cloud Desktop Application version 4.6.1 and earlier versions have Security Bypass vulnerability. Successful exploitation could lead to Privilege Escalation in the context of the current user. CVE ID: CVE-2019-8236	N/A	A-ADO-CREA- 041119/154
experience_n	nanager_form:	<u> </u>			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	22-10-2019	4.3	Adobe Experience Manager Forms versions 6.3-6.5 have a reflected cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. CVE ID: CVE-2019-8089	https://helpx. adobe.com/se curity/produc ts/aem- forms/apsb19 -50.html	A-ADO-EXPE- 041119/155
ant.design					
ant_design_p	ro				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	In Ant Design Pro 4.0.0, reflected XSS in the user/login redirect GET parameter affects the authorization component, leading to execution of JavaScript code in the login after-action script. CVE ID: CVE-2019-18350	N/A	A-ANT-ANT 041119/156
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	e CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
Apache										
traffic_serve	r									
Improper Input Validation	22-10-2019	5	Apache Traffic Server is vulnerable to HTTP/2 setting flood attacks. Earlier versions of Apache Traffic Server didn't limit the number of setting frames sent from the client using the HTTP/2 protocol. Users should upgrade to Apache Traffic Server 7.1.7, 8.0.4, or later versions. CVE ID: CVE-2019-10079				N/A		A-APA-' 041119	
			10079							
thrift										
Loop with Unreachable Exit Condition ('Infinite Loop')	29-10-2019	7.8	version included or click endle with second alread fixed dependent version certain	In Apache Thrift all versions up to and including 0.12.0, a server or client may run into an endless loop when feed with specific input data. Because the issue had already been partially fixed in version 0.11.0, depending on the installed version it affects only certain language bindings.					A-APA-7 041119	
Out-of- bounds Read	29-10-2019	5	In Apache Thrift 0.9.3 to 0.12.0, a server implemented in Go using TJSONProtocol or TSimpleJSONProtocol may panic when feed with invalid input data. CVE ID: CVE-2019-0210			http://m archives he.org/m mbox/th dev/201 mbox/% 7A46CA 4176B11 5D7262	.apac nod_ nrift- .910. .3C27 8749 BBCF	A-APA-7 041119		
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	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
							%40HA0 %3E	GGIS		
poi										
Improper Restriction of XML External Entity Reference ('XXE')	23-10-2019	2.1	when XSSFI conve Micro docur crafte allow files f filesy netwo XML I Proce			N/A		A-APA-I 041119		
Avast										
antivirus										
Untrusted Search Path	23-10-2019	4.4	Avast 19.8 a befor Prelo allow impla %WII bemc loade light; might self-d This a comp e.g., A 19.6.4	An issue was discovered in Avast antivirus before 19.8 and AVG antivirus before 19.8. A DLL Preloading vulnerability allows an attacker to implant %WINDIR%\system32\w bemcomn.dll, which is loaded into a protectedlight process (PPL) and might bypass some of the self-defense mechanisms. This affects all components that use WMI, e.g., AVGSvc.exe 19.6.4546.0 and TuneupSmartScan.dll		N/A		A-AVA- 041119		
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
			CVE ID : CVE-2019- 17093		
AVG	<u>'</u>				
anti-virus					
Untrusted Search Path	23-10-2019	4.4	An issue was discovered in Avast antivirus before 19.8 and AVG antivirus before 19.8. A DLL Preloading vulnerability allows an attacker to implant %WINDIR%\system32\w bemcomn.dll, which is loaded into a protectedlight process (PPL) and might bypass some of the self-defense mechanisms. This affects all components that use WMI, e.g., AVGSvc.exe 19.6.4546.0 and TuneupSmartScan.dll 19.1.884.0. CVE ID: CVE-2019-17093	N/A	A-AVG-ANTI- 041119/162
Broadcom					<u> </u>
network_ope	erations				
Use of Hard- coded Credentials	17-10-2019	6.5	CA Performance Management 3.5.x, 3.6.x before 3.6.9, and 3.7.x before 3.7.4 have a default credential vulnerability that can allow a remote attacker to execute arbitrary commands and compromise system security. CVE ID: CVE-2019-	https://techd ocs.broadcom. com/us/prod uct- content/reco mmended- reading/secur ity- notices/ca- 20191015- 01-security- notice-for-ca-	A-BRO- NETW- 041119/163
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	NCIIPC ID
			13657	performance- management. html	
ca performa	nce_managem	ent		II CIIII	
Use of Hard- coded Credentials	17-10-2019	6.5	CA Performance Management 3.5.x, 3.6.x before 3.6.9, and 3.7.x before 3.7.4 have a default credential vulnerability that can allow a remote attacker to execute arbitrary commands and compromise system security. CVE ID : CVE-2019- 13657	https://techd ocs.broadcom. com/us/prod uct- content/reco mmended- reading/secur ity- notices/ca- 20191015- 01-security- notice-for-ca- performance- management. html	A-BRO-CA_P- 041119/164
Cisco					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	_controller_so	2.1	A vulnerability in the CLI of Cisco Wireless LAN Controller (WLC) Software could allow an authenticated, local attacker to view system files that should be restricted. This vulnerability is due to improper sanitization of user-supplied input in command-line parameters that describe filenames. An attacker could exploit this vulnerability by using directory traversal techniques to submit a path to a desired file location. A successful	N/A	A-CIS-WIRE- 041119/165
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	D	escriptio	otion & CVE ID		Pato	h	NCIIP	C ID
			attacl files t	it could ker to vio that may tive info	ew syste contain	em				
			CVE 1 1526	D : CVE- 66	2019-					
firepower_m	anagement_ce	enter								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interior Firep Center could author attack store (XSS) of the mana The winsuff user-web-interior could vulne malic section that a users could execute code interior would admit to expense in the execute code in the execute	nerabilited manage face of Citower Manager (FMC) allow and crosses attack at exploit exability sious code ons of the crability sious code on a crabili	ement isco anageme Softwar in I, remote nduct a site scrip gainst a sed interface ility is di alidation I input b anageme attacker this by inser e in cert e interfa e to othe essful ex ary scri ontext of ccess wser-ba An attacl alid ccreden	ent e e e e ting user e. ue to of y the ent ting cain ce er ploit cer to pt the sed ker	N/A		A-CIS-F 041119	
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 Dat	te CVSS	·					Pato	h	NCIIP	CID
			CVE I 1528	D : CVE-	2019-						
identity_serv	ices_engin	9	•								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-201	9 3.5	the wimana Cisco Engina an au attack site sea again based interfection of the could vulne persual interfection of the could execute code interfection of the code	ple vulnateblassed gement Identity te (ISE) of thentical error to concripting stauser I manage face. The trabilitie error to care to concripting supplied error to care to classed by I manage face. An analysis adding a face to classed to class	interface Service could all ted, rem nduct cr (XSS) at of the v ement alidation l input th the web ement attacker these s by user of t ick a cra sful expl ne attack crary scri ontext of ccess wser-ba	e of sow note coss-tacks web-e to not hat is content in the content is content in the content is content in the conten	N.	/A		A-CIS-II 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-201	9 3.5	A vulnerability in the web- based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-				N,	/A		A-CIS-II 041119	
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	Descript	ion & CVE I	D	Patc	h	NCIIP	C ID
Scripting')			site scripting against a use based manainterface. To vulnerability insufficient user-supplity processed by based manainterface. A could exploy vulnerability persuading interface to link. A successful allow execute arb code in the interface or sensitive, by information						
			CVE ID : CV 12638	E-2019-					
telepresence	_video_commı	ınicati	on_server						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerabine based manarative interface of Expressway Cisco TeleP Communicative (VCS) could unauthenticattacker to cross-site stattack again web-based interface of system. The is due to installing the validation of the state of the system	agement Cisco Viseries an resence Vintion Serve I allow an cated, rem conduct a cripting (X manageme an affecte e vulnerabe sufficient	d ideo er ote (SS) of the ent d ility	N/A		A-CIS-T 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			mana the af attacl vulne persu interf malic succe allow execu code affect acces	by the vagement offected syker could be rability adding a face to claim should be attacted in the could be seen sitility and the arbitration that arbitration arbitrat	interfacystem. And exploit by user of to ick and cker to cary scripton face or we brow	e of in this the ld pt the				
			1270	D : CVE	2019-					
telepresence	_collaboration	_endp	•	nle vuln	erahiliti	es in				
Improper Privilege Managemen t	16-10-2019	6.6	the C TeleF Collai (CE): an au attacl arbiti vulne insufi enfor could vulne authe remo subm to spe succe allow overv	Multiple vulnerabilities in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to overwrite arbitrary files. The vulnerabilities are due to insufficient permission enforcement. An attacker could exploit these vulnerabilities by authenticating as the remote support user and submitting malicious input to specific commands. A successful exploit could allow the attacker to overwrite arbitrary files on the underlying					A-CIS-T 041119	
CV Scoring Sca	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	Description & CVE ID				Pato	:h	NCIIP	CID	
				conte writt Overv could crash of ser	o controents of the en to the writing at lease the control con	e data e file. a critical ne devic ng in a d dition (file e to enial					
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	16-	10-2019	7.2	of Cis Collai (CE) an au attack comm vulned insuff validate could vulned auther admi withing and se input comm explor attack previ- from filesy	nerability co Telef boration Software thentica ker to pe nand inje erability ficient in ation. An exploit erability enticatin nistrativ n the res ubmittir to a spe nand. A s oit could ker to ex ously sta the unde stem. ID: CVE-	Presence Endpoi e could a ted, loca erform ections. is due to aput attacke this by g as an e level u etricted s ag malici cific successfi allow th ecute aged cod erlying	nt lllow ll The o r shell ious ul e	N/	Ά		A-CIS-T 041119	
Improper Privilege Managemen t	16-	10-2019	7.2	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to execute				N/	A		A-CIS-T 041119	
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
			arbitrary commands with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating as the remote support user and submitting malicious input to a specific command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system (OS) with root privileges. CVE ID: CVE-2019-15275		
Improper Privilege Managemen t	16-10-2019	7.2	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to execute code with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating as the remote support user and sending malicious traffic to a listener who is internal to the device. A successful exploit could allow the attacker to execute commands with	N/A	A-CIS-TELE- 041119/173

Weakness	Publish D	ate	cvss	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
				_	orivilege D : CVE - 7						
Incorrect Default Permissions	16-10-20		6.6	Collaboration (CE) So an aurattack the /r affect vulne assign could vulne as the and w /root affect CVE I 1596	of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an affected device. CVE ID: CVE-2019- 15962			N/A		A-CIS-T 041119	
identity_serv	ices_engi	ne_so	oftwar	e							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-20)19	3.5	based interf Service Softw auther attack stored (XSS) of the mana an aff attack admin The vinsuff				N/A		A-CIS-II 041119	
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	

Missing Authentication for Critical Function Missing Function Missing Authentication for Critical Function Missing Function Critical Function Missing Authentication for Critical Function Missing Authentication Logic of the web-based management interface. An antacker could exploit this vulnerability by sending a crafted request to the web interface. As successful exploit could allow the attacker to read a tepdump file generated with a particular naming scheme. CVE ID: CVE-2019-15282	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIP	C ID
Missing Authentication on for Critical Function 16-10-2019 16-10-2019 5 based management interface of Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker read tcpdump files generated on an affected device. The vulnerability is due an issue in the authentication logic of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web interface. A successful exploit could allow the attacker to read a tcpdump file generated with a particular naming scheme. CVE ID: CVE-2019-				interface of the affected software. An attacker could exploit this vulnerability by injecting malicious code into a troubleshooting file. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browserbased information. CVE ID: CVE-2019-			
	Authenticati on for Critical	16-10-2019	5	based management interface of Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker read tcpdump files generated on an affected device. The vulnerability is due an issue in the authentication logic of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web interface. A successful exploit could allow the attacker to read a tcpdump file generated with a particular naming scheme. CVE ID: CVE-2019-	N/A		

Weakness	Pul	blish Date	e CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
Cmsmadesim	ple										
cms_made_si	mpl	e									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	(CMS store a craft on thuploa	d XSS by ted image e "file m id image D : CVE	11 allow an adm ge filena anager > s" scree	in via me	N/A		A-CMS-041119	_
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	(CMS store a craf on th Articl	d XSS by ted imag e "News le" scree D : CVE	11 allow an adm ge filena > Add n.	in via	N/A		A-CMS-041119	_
Codesys											
eni_server											
Out-of- bounds Write	25-	10-2019	7.5	up to Buffe	V3.2.2.2 r Overflo T D : CVE	ow.	rver	https://mers.com/file n/data/omers/se /2019/A ry2019- 09_LCDS 319.pdf	desys. admi custo curity ddviso	A-COD-: 041119	_
codesys											
Out-of- bounds Write	25-	10-2019	7.5	up to Buffe	V3.2.2.2 r Overflo T D : CVE	ow.	rver	https://mers.com/file n/data/omers/se /2019/A ry2019- 09_LCDS	desys. admi custo curity ddviso	A-COD-041119	
CV Scoring Scal	le	0-1	1-2	2-3	3-4	3-4 4-5 5-6		6-7	7-8	8-9	9-10

Weakness	Publi	sh Date	CVSS	D	escriptio	n & CVE I	D	Pate	ch	NCIIF	CID
								319.pdf			
corehr											
core_portal											
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	25-10)-2019	4.3	27.0.7 CVE I	CoreHR Core Portal before 27.0.7 allows stored XSS. CVE ID: CVE-2019- 18221			N/A		A-COR- 041119	
Craftcms											
craft_cms											
Weak Password Recovery Mechanism for Forgotten Password	24-10)-2019	5	the el passy being norm leadin of a b them	D : CVE	ession ompt wa nited like forms, possibi ce attem	s not	N/A		A-CRA-041119	
cybelsoft											
thinvnc											
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-10)-2019	5	ThinVNC 1.0b1 is vulnerable to arbitrary file read, which leads to a compromise of the VNC server. The vulnerability exists even when authentication is turned on during the deployment of the VNC server. The password for authentication is stored in cleartext in a file that can be read via a			N/A		A-CYB-' 041119		
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Dat	ce CVSS	•			D		Pato	h	NCIIP	C ID
				'hinVnc.i rsal atta		•					
			CVE I 1766	D : CVE- 2	-2019-						
darktrace											
enterprise_ir	nmune_sys	tem									
Cross-Site Request Forgery (CSRF)	23-10-201	9 4.3	Immı allow	crace Entrage	em befor via the	re 3.1	N,	/A		A-DAR- 041119	
			CVE I	D : CVE	-2019-9	596					
Cross-Site Request Forgery (CSRF)	23-10-201	9 4.3	Darktrace Enterprise Immune System before 3.1 allows CSRF via the /config endpoint.		N/A		A-DAR- 041119				
(dorar)			CVE ID : CVE-2019-9597								
dkd											
direct_mail											
Information Exposure	16-10-201	9 4	The direct_mail (aka Direct Mail) extension through 5.2.2 for TYPO3 has a missing access check in the backend module, allowing a user (with restricted permissions to the fe_users table) to view and export data of frontend users who are subscribed to a newsletter.				or ac 3-	ttps://r rg/secu lvisory -ext-sa- 019-01	rity/ /typo	A-DKD- 041119	
			1669	8							
doas_project											
doas					1.	1 .					
N/A	18-10-201	9 10	An issue was discovered in slicer69 doas before 6.2 on certain platforms other			N,	/A		A-DOA- 041119		
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6			5-6		6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			than OpenBSD. On platforms without strtonum(3), sscanf was used without checking for error cases. Instead, the uninitialized variable errstr was checked and in some cases returned success even if sscanf failed. The result was that, instead of reporting that the supplied username or group name did not exist, it would execute the command as root. CVE ID: CVE-2019-15900			
Improper Input Validation	18-10-2019	9	An issue was discovered in slicer69 doas before 6.2 on certain platforms other than OpenBSD. A setusercontext(3) call with flags to change the UID, primary GID, and secondary GIDs was replaced (on certain platforms: Linux and possibly NetBSD) with a single setuid(2) call. This resulted in neither changing the group id nor initializing secondary group ids. CVE ID: CVE-2019-15901	N/A	A-DOA-DOAS- 041119/188	
Dolibarr						
dolibarr					1.50.	
Improper Neutralizati	16-10-2019	3.5	An issue was discovered in Dolibarr 10.0.2. It has XSS	N/A	A-DOL-DOLI- 041119/189	
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	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
on of Input During Web Page Generation ('Cross-site Scripting')			setup /adm edit U email recipi	e "outgo " feature in/mails IRI via th s to (ins ents, for oses)" fie	e in the s.php?ac ne "Send tead of r	tion= all				
			CVE I 1757	D : CVE- 6	2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Dolib via th setup admin dit UI for er (field email	sue was arr 10.0 e "outgo" feature n/mails. RI via the ror retus s 'Errors s sent)" D: CVE-7	2. It has ping emand in the php?act e "Email rns emands-To' in field.	XSS ail ion=e used	N/A		A-DOL-I 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Dolib via th setup admir dit UI email (defa	An issue was discovered in Dolibarr 10.0.2. It has XSS via the "outgoing email setup" feature in the admin/mails.php?action=e dit URI via the "Sender email for automatic emails (default value in php.ini: Undefined)" field. CVE ID: CVE-2019-					A-DOL-I 041119	
dormsystem	_project									
dormsystem Improper				1	-					
Neutralizati on of Input During Web Page Generation	24-10-2019	4.3	tonyy dormsystem through 1.3 allows DOM XSS. CVE ID: CVE-2019- 17581				N/A		A-DOR- DORM- 041119/192	
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	D	escriptio	n & CVE I	D	Pate	h	NCIIP	PC ID
('Cross-site Scripting')										
Eclipse										
openj9										
Incorrect Permission Assignment for Critical Resource	17-10-2019	6.4	to 0.1 diagn as cau a diag perm privil	Eclipse 6, access ostic op using a G gnostic fi itted wit ege chec 1	s to erations C or cre ile are thout an	such ating	https:// clipse.or gs/show cgi?id=5	g/bu _bug.	A-ECL-0 041119	
wild_web_de	veloper									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	4	XMLLanguageService.java in XML Language Server (aka lsp4xml) before 0.9.1, as used in Red Hat XML Language Support (aka vscode-xml) before 0.9.1 for Visual Studio and other products, allows a remote attacker to write to arbitrary files via Directory Traversal. CVE ID: CVE-2019-				https:// b.com/a zerr/lsp blob/ma CHANGI md#oth	ngelo 4xml/ aster/ ELOG.	A-ECL-\ 041119	
XML Injection (aka Blind XPath Injection)	23-10-2019	6.5	XML Language Server (aka lsp4xml) before 0.9.1, as used in Red Hat XML Language Support (aka vscode-xml) before 0.9.1 for Visual Studio and other products, allows XXE via a crafted XML document, with resultant SSRF (as well as SMB connection initiation that can lead to NetNTLM				https:// b.com/a zerr/lsp blob/ma CHANGI md#oth	ngelo 4xml/ aster/ ELOG.	A-ECL-\ 041119	
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	Puk	olish Date	cvss	SS Description & CVE ID		D	l	Patc	h	NCIIP	C ID	
				captu crack exten parti	enge/restre for parting). The sions/cocipants/ILParser	assword is occurs ontentm diagnos	s in odel/ tics/L					
				CVE 1 1821	ID : CVE	-2019-						
eq-3												
cux-daemon												
Improper Control of Generation of Code ('Code Injection')	17-3	10-2019	9	(RCE) CUx-1 eQ-3 Firm 2.45.4 author executas root simpl	_	n the add 1.11a of atic CCU 5.16 und remote I attacked m communication request.	the til ers to	N/A			A-EQ0 041119	
Information Exposure	17-2	10-2019	4	A Localissue Daem Homo 2.35. remo attacl files v Requ CVE I	CVE ID: CVE-2019-14423 A Local File Inclusion (LFI) issue in the addon CUx-Daemon 1.11a of the eQ-3 Homematic CCU-Firmware 2.35.16 until 2.45.6 allows remote authenticated attackers to read sensitive files via a simple HTTP Request. CVE ID: CVE-2019-14424		N/A			A-EQ0 041119		
etherpad												
etherpad							1				. ==	
Improper Neutralizati	19-1	10-2019	4.3	templates/pad.html in Etherpad-Lite 1.7.5 has				A-ETH- 041119				
CV Scoring Sca (CVSS)	ıle	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
on of Input During Web Page Generation ('Cross-site Scripting') eu_cookie_la			XSS when the browser does not encode the path of the URL, as demonstrated by Internet Explorer. CVE ID: CVE-2019-18209		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	The eu-cookie-law plugin through 3.0.6 for WordPress (aka EU Cookie Law (GDPR)) is susceptible to Stored XSS due to improper encoding of several configuration options in the admin area and the displayed cookie consent message. This affects Font Color, Background Color, and the Disable Cookie text. An attacker with high privileges can attack other users. CVE ID: CVE-2019-16522	N/A	A-EUEU_C- 041119/199
file_project					
file					
Out-of- bounds Write	21-10-2019	7.5	cdf_read_property_info in cdf.c in file through 5.37 does not restrict the number of CDF_VECTOR elements, which allows a heap-based buffer overflow (4-byte out-of-bounds write). CVE ID: CVE-2019-	N/A	A-FIL-FILE- 041119/200
CV Scoring Sca	l le				
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-1 0

Weakness	Publish Date	cvss	Description & CVE ID	Patch	n	NCIIPO	CID
			18218				
forcepoint							
one_endpoin	t						
Incorrect Authorizatio n	23-10-2019	4	This vulnerability allows a normal (non-admin) user to disable the Forcepoint One Endpoint (versions 19.04 through 19.08) and bypass DLP and Web protection. CVE ID: CVE-2019-6144	N/A		A-FOR-0 041119/	_
Fortinet							
forticlient							
Uncontrolle d Search Path Element	24-10-2019	4.4	A malicious DLL preload vulnerability in Fortinet FortiClient for Windows 6.2.0 and below allows a privileged attacker to perform arbitrary code execution via forging that DLL. CVE ID: CVE-2019-6692	N/A		A-FOR-F 041119/	_
Foxitsoftwar	e						
foxit_studio_	photo						
Out-of- bounds Read	25-10-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information 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 conversion from JPEG to	N/A		A-FOX-F 041119,	
CV Scoring Sca (CVSS)	lle 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Des	scription	n & CVE I	D	Pato	h	NCIIP	C ID
			from the validate data, we read parallocate attacked in conjuction code in	ne lack ion of the hich can est the ed stru er can le unction abilities the co t proce 309.	e results of proposition user-sup an result end of a cture. A everage n with or s to execute ntext of ss. Was	er oplied t in a n this ther cute				
foxit_reader										
Out-of- bounds Write	25-10-2019	6.8	remote execute affected Foxit P 9.5.0.20 interace exploit in that visit a ropen a specific the producer HTML2 issue resof propuser-sucan resorthe encoopiect. leverage to execute context.	e attack e arbitr d instal hanton 0723. Ution is this vulte tarmalicio malicio c flaw e ocessing ript in the 2PDF plesults for valicult in a d of an attage this vute coot of the	rary cod llations nPDF Jser required alnerabi get mus us page ous file. exists wi	e on of d to lity of The thin he e lack of chich past d n poility	N/A		A-F0X-I 041119	
CV Scoring Sca	le 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 8	& CVE ID	Pato	h	NCIIP	C ID
			8692. CVE ID : CVE-20 17139	019-				
phantompdf								
Out-of- bounds Write	25-10-2019	6.8	This vulnerability remote attacker execute arbitrary affected installary foxit Phantom P. 9.5.0.20723. Use interaction is receptoit this vulning that the target visit a malicious open a malicious specific flaw exist the processing of Javascript in the HTML2PDF plugissue results from of proper validation user-supplied docan result in a with end of an all object. An attackleverage this vulto execute code context of the comprocess. Was ZE 8692.	rs to ry code on tions of PDF er equired to herability et must s page or s file. The sts within of e gin. The om the lack etion of hata, which vrite past hocated ker can lnerability in the hurrent DI-CAN-	N/A		A-FOX-F 041119	
			17139 This vulnerabili	-				
Use After Free	25-10-2019	6.8	remote attacker execute arbitrar affected installa Foxit Phantom P 9.6.0.25114. Use interaction is reexploit this vuln	N/A		A-FOX-I 041119		
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	D	escription	n & CVE II	D	Pate	ch	NCIIP	C ID
			visit a open specification open specification of the observation of the observation open specification open	t the tar malicio a malicio a malicio ic flaw e andling c cus even ts from t ating the ject prio rming op ject. An age this v ecute coc xt of the ss. Was D: CVE-	us page ous file. 'exists wi of the ot. The is he lack of existency attacker wilnerable in the current ZDI-CAN	or The thin sue of ce of r can oility				
Use After Free	25-10-2019	6.8	remote execular affect Foxit 9.6.0.1 interaction in that visit a open specific the provided an object of the object of executive executi	vulnerabe te attack te arbitred instal Phanton 25114. Unction is a malicion a malicion a malicion a Calculat field. Es from the ting the piect priorming oppiect. An age this vecute coext of the	ters to cary code ary code ary code ary code ary code are are are are are are are are are ar	e on of d to dity t or The thin ot ion ie of ce of s on r can oility	N/A		A-FOX-I 041119	
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	Pu	blish Date	CVSS	D	escriptio	n & CVE I	D	Pato	ch	NCIIP	CID
				9044 CVE I 1714	D : CVE	-2019-					
Use After Free	25-	10-2019	6.8	remo executaffect Foxit 9.6.0. interaction in that visit a open specific the provided an object of a literation of a literatio	D : CVE-	ters to cary cod llations mPDF Jser required linerabing the must be susted with the lack of existen or to peration attacked vulneral de in the Edit CAN	e on of d to lity t or The thin pt tion issue of ce of as on or can oility	N/A		A-FOX-I 041119	
Use After Free	25-	10-2019	4.3	remo disclo informatal Phane User a requi	vulnerab te attack ose sensi mation o lations o tomPDF interacti red to ex	tive on affector for affector for for for for for for for for for f	ed 114. is	N/A		A-FOX-I 041119	
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
			malic malic flaw e parsin issue of val of an perfo the ol levera conju vulne code i curre CAN-O		The specthin the VG files. If the exist rior to be be be attacked	The lack ence s on r can er cute the				
			1714	D : CVE- 3	2019-					
Out-of- bounds Write	25-10-2019	6.8	remore executa affect Foxit 9.6.0. interaction in that wisit a open specific the confiles the co	vulnerabete attack te arbitred instale Phanton 25114. Unaction is it this vultation a malicion a malicion a malicion o PDF. Totale from the validation a writer validation a writer and allocure. An allocure. An allocure cooxt of the	ters to cary code lations of PDF Jser required linerability get mus us page ous file. It is to nof DW he issue the lack of the past to cated attacker wulnerabile in the	e on of d to dity t or The thin G of ser- can che	N/A		A-F0X-I 041119	
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	Pato	ch	NCIIP	CID
			process. Was ZDI-CAN- 9274. CVE ID : CVE-2019- 17144				
Out-of- bounds Write	25-10-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 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 conversion of DXF files to PDF. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9276. CVE ID: CVE-2019-17145	N/A		A-F0X-F 041119	
Freepbx							
contactmana	ger		An icono rusa disassessa disa				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	21-10-2019	4.3	An issue was discovered in Contactmanager 13.x before 13.0.45.3, 14.x before 14.0.5.12, and 15.x before 15.0.8.21 for FreePBX 14.0.10.3. In the Contactmanager class	N/A		A-FRE-0 041119	
CV Scoring Sca (CVSS)	o-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Pul	olish Date	CVS	S D	escription	n & CVE I	D		Pato	h	NCIIP	PC ID
Scripting')				ntact nager unsar comit reflec occas It can GET 1 /adm conta	Nadmin manager c.class.phoitized grom for ted in Hosions, lead in Hosions, lead in Jana, lactmanage (D: CVE-166)	TContaction (Contaction), and the URL TML on ding to Contaction (Contaction) and the Contactio	riable is 2 XSS. a a					
freepbx												
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-	10-2019	4.3	Conta before before Free Free Free Free Free Free Free F	sue was eactmanage 13.0.4. PBX 14.0 actmanager c.class.phaitized grom fitted in Histons, lead to be request the complete that the complete	ger 13.x 5.3, 14.x 12, and 21 for .10.3. In ger class module Contact np), an roup van the URL TML on ding to 2 ested vi o php?mod ger.	the ses\coctma riable is 2 XSS. a a	N/A			A-FRE-1 041119	
Improper Neutralizati on of Input During Web Page Generation	21-	10-2019	4.3	Mana 13.0.: 15.0.: 14.0.:	An issue was discovered in Manager 13.x before 13.0.2.6 and 15.x before 15.0.6 before FreePBX 14.0.10.3. In the Manager module form						A-FRE-l 041119	
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	D	escriptio	n & CVE I	D		Patc	h	NCIIF	PC ID
('Cross-site Scripting')			anage an un mana comin reflect to XSS via GI /conf play=	(html\admin\modules\m anager\views\form.php), an unsanitized managerdisplay variable coming from the URL is reflected in HTML, leading to XSS. It can be requested via GET request to /config.php?type=tool&dis play=manager. CVE ID: CVE-2019- 16967							
manager											
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	Mana 13.0.2 15.0.6 14.0.2 modu (html anage an un mana comin reflect to XS2 via GI /conf play=	ger 13.x 2.6 and 1 5 before 10.3. In the form hadmin er views sanitize gerdisplated in H S. It can ET reque ig.php?t manage D: CVE- 7	before 5.x before FreePB he Mana module form.p d ay varia the URL TML, lea be reque est to ype=too r.	ore K ager es\m hp), ble is ading ested	N/A			A-FRE- 041119	
fusionpbx											
fusionpbx											
Improper Neutralizati on of Special Elements in Output Used by a	21-10-2019	9	app/call_centers/cmd.php in the Call Center Queue Module in FusionPBX up to 4.5.7 suffers from a command injection vulnerability due to a lack			N/A			A-FUS-1 041119		
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	NCIIPC ID
Downstrea m Component ('Injection')			of input validation, which allows authenticated attackers (with at least the permission call_center_queue_add or call_center_queue_edit) to execute any commands on the host as www-data. CVE ID: CVE-2019-16964		
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component ('Injection')	21-10-2019	9	resources/cmd.php in FusionPBX up to 4.5.7 suffers from a command injection vulnerability due to a lack of input validation, which allows authenticated administrative attackers to execute any commands on the host as www-data. CVE ID: CVE-2019- 16965	N/A	A-FUS-FUSI- 041119/217
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	An issue was discovered in FusionPBX up to 4.5.7. In the file app\conference_controls\ conference_control_details .php, an unsanitized id variable coming from the URL is reflected in HTML on 2 occasions, leading to XSS. CVE ID: CVE-2019-	N/A	A-FUS-FUSI- 041119/218
Improper Neutralizati on of Input During Web Page	21-10-2019	4.3	In FusionPBX up to 4.5.7, the file app\fifo_list\fifo_interacti ve.php uses an unsanitized "c" variable coming from	N/A	A-FUS-FUSI- 041119/219

Weakness	Pul	olish Date	е	CVSS	D	escription	n & CVE I	D		Pato	:h	NCII	PC ID
Generation ('Cross-site Scripting')					in HT	RL, whic ML, lead D : CVE- 9	ing to X						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-	10-2019)	4.3	In FusionPBX up to 4.5.7, the file app\sip_status\sip_status. php uses an unsanitized "savemsg" variable coming from the URL, which is reflected in HTML, leading to XSS. CVE ID: CVE-2019-16970 In FusionPBX up to 4.5.7,					/A		A-FUS- 04111	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	22-	10-2019)	4.3	the fill app\1 hread unsar varial URL, 3 occar leading	the file app\messages\messages_t hread.php uses an unsanitized "contact_uuid" variable coming from the URL, which is reflected on 3 occasions in HTML, leading to XSS. CVE ID: CVE-2019-				/A		A-FUS- 04111	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	22-	10-2019)	4.3	the fill app\c resserunsar comir which HTMI	In FusionPBX up to 4.5.7, the file app\contacts\contact_add resses.php uses an unsanitized "id" variable coming from the URL, which is reflected in HTML, leading to XSS. CVE ID: CVE-2019-16972			N,	/A		A-FUS- 04111	
Improper Neutralizati on of Input During Web	22-:	10-2019)	4.3	In FusionPBX up to 4.5.7, the file app\contacts\contact_edit .php uses an unsanitized			N,	/A		A-FUS- 04111		
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	Pul	blish Date	е	CVSS	D	escriptio	n & CVE I	D		Pato	h	NCIIF	PCID
Page Generation ('Cross-site Scripting')					comir which HTMI	y_string ng from t n is refle L, leading	the URL, cted in g to XSS	•					
					CVE I 1697	D : CVE- 3	2019-						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-	10-2019)	4.3	the URL, which is reflected in HTML, leading to XSS. CVE ID: CVE-2019- 16974					/A		A-FUS-1 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-	10-2019)	4.3	In FusionPBX up to 4.5.7, the file app\contacts\contact_not es.php uses an unsanitized "id" variable coming from the URL, which is reflected in HTML, leading to XSS. CVE ID: CVE-2019-				N	/A		A-FUS-1 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-	10-2019)	4.3	In Fusthe file app\c ion_ir unsar varial URL, varial leadir	In FusionPBX up to 4.5.7, the file app\destinations\destinat ion_imports.php uses an unsanitized "query_string" variable coming from the URL, which is reflected on 2 occasions in HTML, leading to XSS. CVE ID: CVE-2019-16976			N	/A		A-FUS-1 041119	
Improper Neutralizati on of Input During Web	23-	10-2019	9	4.3	In FusionPBX up to 4.5.7, the file app\extensions\extension _imports.php uses an			N	/A		A-FUS-1 041119		
CV Scoring Sca (CVSS)	le	0-1	1	1-2	2-3	3-4	4-5	5-6		6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Des	scription	n & CVE I	D	Pato	:h	NCIIP	C ID
Page Generation ('Cross-site Scripting')			variabl URL, w	e comi hich is	query_st ng from reflecte g to XSS	the ed in				
			CVE ID 16977	_	2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	the file app\de gs.php "id" van the UR	evices\ uses and a seriable of the control of the c		settin itized from ected	N/A		A-FUS-F 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	the file app\co.php us "id" var the UR in HTM	ontacts\ ses an u riable o L, whic IL, lead : CVE -	up to value on tack the coming of the coming to X 2019-	t_urls zed from ected	N/A		A-FUS-F 041119	
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	21-10-2019	6.5	In FusionPBX up to v4.5.7, the file app\call_broadcast\call_br oadcast_edit.php uses an unsanitized "id" variable coming from the URL in an unparameterized SQL query, leading to SQL injection. CVE ID: CVE-2019-16980				N/A		A-FUS-F 041119	
Improper Neutralizati on of Input	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\conference_profiles\c			N/A		A-FUS-F 041119		
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	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			onference_profile_params. php uses an unsanitized "id" variable coming from the URL, which is reflected on 2 occasions in HTML, leading to XSS. CVE ID: CVE-2019-		
			16981		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\access_controls\acces s_control_nodes.php uses an unsanitized "id" variable coming from the URL, which is reflected in HTML, leading to XSS. CVE ID: CVE-2019-16982	N/A	A-FUS-FUSI- 041119/232
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file resources\paging.php has a paging function (called by several pages of the interface), which uses an unsanitized "param" variable constructed partially from the URL args and reflected in HTML, leading to XSS. CVE ID: CVE-2019-16983	N/A	A-FUS-FUSI- 041119/233
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\recordings\recording _play.php uses an unsanitized "filename" variable coming from the URL, which is base64 decoded and reflected in	N/A	A-FUS-FUSI- 041119/234

Weakness	Publis	sh Date	CVSS	D	escriptio	n & CVE I	D	Pat	tch	NCIIP	CID
				HTMI	L, leadin	g to XSS					
				CVE I 1698	D : CVE- 4	2019-					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-10	0-2019	8.5	the fil app\x te.php "rec" the Ut decod deleti system	xml_cdr\ o uses ar variable RL, whice led and a on of an m. D: CVE-	xml_cdi n unsani coming h is base allows y file of	c_dele tized from e64	N/A		A-FUS-F 041119	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-10	0-2019	4	In FusionPBX up to v4.5.7, the file resources\download.php uses an unsanitized "f" variable coming from the URL, which takes any pathname and allows a download of it. (resources\secure_downlo ad.php is also affected.) CVE ID: CVE-2019-16986				N/A		A-FUS-F 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10)-2019	4.3	In FusionPBX up to v4.5.7, the file app\contacts\contact_imp ort.php uses an unsanitized "query_string" variable coming from the URL, which is reflected in HTML, leading to XSS. CVE ID: CVE-2019-16987			N/A		A-FUS-F 041119		
Improper Neutralizati on of Input	21-10)-2019	4.3	In FusionPBX up to v4.5.7, the file app\basic_operator_panel			N/A		A-FUS-F 041119		
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	D	escription	n & CVE I	D	Pa	itch	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			uses a "eave comin which occas	urces\co an unsan sdrop_d ng from t n is refle ions in F ng to XSS	itized est" vari the URL, cted on 1	iable				
			CVE I 1698	D : CVE- 8	2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	the fil app\c onfer uses a varial URL, HTMI	conferen ence_int an unsan ole comi which is _, leading D: CVE-	ces_acti eractive litized "o ng from reflecte g to XSS.	ve\c .php c" the d in	N/A		A-FUS-I 041119	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-10-2019	4	the fil app/r _on_h unsar comir which (base allow	In FusionPBX up to v4.5.7, the file app/music_on_hold/music _on_hold.php uses an unsanitized "file" variable coming from the URL, which takes any pathname (base64 encoded) and allows a download of it. CVE ID: CVE-2019-					A-FUS-I 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\edit\filedelete.php uses an unsanitized "file" variable coming from the URL, which is reflected in HTML, leading to XSS. CVE ID: CVE-2019-16991				N/A		A-FUS-I 041119	
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 Da	ate	CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
GNU											
guix											
Incorrect Permission Assignment for Critical Resource	17-10-202	19	4.6	local to an accourage user-yworld issue	Guix 1.0. users to arbitrar, nt becaunt directo profile do CVE-2 D: CVE-2	gain acc y user's use the ory of th irectoric e, a simi	ess e es is ilar	N/A		A-GNU- 041119	
libidn2					18192						
Improper Input Validation	22-10-203	19	5	fails to round in RF6 when to U-l possible circum doma anoth malic match exceptor certain Unicol would conver Unicol back farbitr	GNU libidn2 before 2.2.0 fails to perform the roundtrip checks specified in RFC3490 Section 4.2 when converting A-labels to U-labels. This makes it possible in some circumstances for one domain to impersonate another. By creating a malicious domain that matches a target domain except for the inclusion of certain punycoded Unicode characters (that would be discarded when converted first to a Unicode label and then back to an ASCII label), arbitrary domains can be impersonated.		https://com/lib bidn2/c t/61413 4c60e19 42e3ed3 8d389d	idn/li commi 17ef6e 950d7 f0a0ef	A-GNU- 041119		
Out-of- bounds Write	21-10-202	19	7.5	idn2_to_ascii_4i in lib/lookup.c in GNU libidn2 before 2.1.1 has a			N/A		A-GNU- 041119		
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	D	escriptio	n & CVE	D	Pato	h	NCIIP	C ID
			overf doma	based b low via a nin string	a long g.					
goharbor			18224							
harbor										
Incorrect Default Permissions	18-10-2019	5	Access vulne vulne proje use tl creat with and/o perm they contr API d prope perm scope to cre accou	D : CVE	The allows nistrator or API to t account rized pu ccess to a proj we acces the Harb aforce the and proj API requ w robot	rs to it ish ect s or or ne ect	http://w mware.c ecurity/ ories/VN 2019- 0016.htm	om/s advis MSA-	A-GOH- 041119	
Golang										
go							h44	aitle -		
Interpretati on Conflict	24-10-2019	5	Go before 1.12.11 and 1.3.x before 1.13.2 can panic upon an attempt to process network traffic containing an invalid DSA public key. There are several attack scenarios, such as traffic from a client to a server that verifies		https://s b.com/g /go/issu 4960, https://s s.google. d/msg/g - announc m7llp0w	olang les/3 group com/ golang	A-GOL-0 041119			
CV Scoring Sca (CVSS)	lle 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
			client certificates. CVE ID : CVE-2019- 17596	afyRkgCgAJ	
Haproxy					
haproxy					
Improper Input Validation	23-10-2019	4.3	A flaw was found in HAProxy before 2.0.6. In legacy mode, messages featuring a transferencoding header missing the "chunked" value were not being correctly rejected. The impact was limited but if combined with the "http-reuse always" setting, it could be used to help construct an HTTP request smuggling attack against a vulnerable component employing a lenient parser that would ignore the content-length header as soon as it saw a transfer-encoding one (even if not entirely valid according to the specification). CVE ID: CVE-2019-18277	N/A	A-HAP-HAPR- 041119/247
hcltech					
traveler					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	18-10-2019	3.5	HCL Traveler versions 9.x and earlier are susceptible to cross-site scripting attacks. On the Problem Report page of the Traveler servlet pages, there is a field to specify a file attachment to provide	https://hclpn psupport.hclt ech.com/csm? id=kb_article &sysparm_art icle=KB00732	A-HCL-TRAV- 041119/248
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	NCIIPC ID
Scripting')			additional problem details. An invalid file name returns an error message that includes the entered file name. If the file name is not escaped in the returned error page, it could expose a cross-site scripting (XSS) vulnerability. CVE ID: CVE-2019-4409		
hexo-admin_	project				
hexo-admin					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	The Post editor functionality in the hexo- admin plugin versions 2.3.0 and earlier for Node.js is vulnerable to stored XSS via the content of a post. CVE ID: CVE-2019- 17606	https://www. npmjs.com/ad visories/1211	A-HEX-HEXO- 041119/249
hongcms_pro	ject				
hongcms					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	HongCMS 3.0.0 has XSS via the install/index.php servername parameter. CVE ID: CVE-2019-17607	N/A	A-HON- HONG- 041119/250
Improper Neutralizati on of Input During Web Page Generation	16-10-2019	4.3	HongCMS 3.0.0 has XSS via the install/index.php dbname parameter. CVE ID: CVE-2019-17608	N/A	A-HON- HONG- 041119/251
CV Scoring Sca (CVSS)	o-1	1-2	2-3 3-4 4-5 5-6 98	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	HongCMS 3.0.0 has XSS via the install/index.php dbusername parameter. CVE ID: CVE-2019-17609	N/A	A-HON- HONG- 041119/252
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	HongCMS 3.0.0 has XSS via the install/index.php dbpassword parameter. CVE ID: CVE-2019-17610	N/A	A-HON- HONG- 041119/253
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	HongCMS 3.0.0 has XSS via the install/index.php tableprefix parameter. CVE ID: CVE-2019-17611	N/A	A-HON- HONG- 041119/254
Horde					
groupware			-		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	4.3	Horde Groupware Webmail Edition through 5.2.22 allows XSS via an admin/user.php?form=up date_f&user_name= or admin/user.php?form=re move_f&user_name= or admin/config/diff.php?ap p= URI, related to the Tag Cloud feature. CVE ID: CVE-2019-	N/A	A-HOR-GROU- 041119/255
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
			12094		
Cross-Site Request Forgery (CSRF)	24-10-2019 6.8		Horde Trean, as used in Horde Groupware Webmail Edition through 5.2.22 and other products, allows CSRF, as demonstrated by the treanBookmarkTags parameter to the trean/ URI on a webmail server.	N/A	A-HOR-GROU- 041119/256
			CVE ID : CVE-2019- 12095		
hornerauton	nation				
cscape					
Improper Input Validation	18-10-2019	6.8	In Horner Automation Cscape 9.90 and prior, an improper input validation vulnerability has been identified that may be exploited by processing files lacking user input validation. This may allow an attacker to access information and remotely execute arbitrary code. CVE ID: CVE-2019-13541	N/A	A-HOR-CSCA- 041119/257
Out-of- bounds Write	18-10-2019	6.8	In Horner Automation Cscape 9.90 and prior, improper validation of data may cause the system to write outside the intended buffer area, which may allow arbitrary code execution. CVE ID: CVE-2019- 13545	N/A	A-HOR-CSCA- 041119/258
hotel_and_lo	dge_managem	ent_sys	stem_project		
CV Scoring Sca	ale 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		
hotel_and_lo	dge_managem	ent_sys	stem				
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	23-10-2019	7.5	Sourcecodester Hotel and Lodge Management System 1.0 is vulnerable to unauthenticated SQL injection and can allow remote attackers to execute arbitrary SQL commands via the id parameter to the edit page for Customer, Room, Currency, Room Booking Details, or Tax Details. CVE ID: CVE-2019-	N/A	A-HOT-HOTE- 041119/259		
			18387				
IBM	udium bia dat	a intal	Lacus				
security_gua	rdium_big_dat	a_intei	<u> </u>		T		
Exposure of Resource to Wrong Sphere	29-10-2019	6.4	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 specifies permissions for a security- critical resource which could lead to the exposure of sensitive information or the modification of that resource by unintended parties. IBM X-Force ID: 160986.	https://www. ibm.com/sup port/pages/n ode/1096396	A-IBM-SECU- 041119/260		
			CVE ID : CVE-2019-4306				
Insufficientl y Protected Credentials	29-10-2019	2.1	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 160987. CVE ID: CVE-2019-4307	https://www. ibm.com/sup port/pages/n ode/1096288	A-IBM-SECU- 041119/261		
Use of Hard-	29-10-2019	2.1	1 IBM Security Guardium https://www. A-IBM-SECU-				
CV Scoring Sca (CVSS)	lle 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
coded Credentials			(Sona coded could obtain inform ID: 16	d creden allow a n highly mation. l	ligence uses har tials wh local use sensitiv IBM X-Fo	ich er to e orce	ibm.com port/pag ode/109	ges/n	041119	/262
Information Exposure	29-10-2019	5	Big D (Sona sensiti unauti inform mour the sy ID: 16	ata IntelarG) 4.0 (tive info thorized mation c at furthe ystem. IE	Guardiu ligence discloses rmation users. T ran be us r attacks BM X-For	to The Sed to Son rce	https://ibm.com port/pag ode/109	/sup ges/n	A-IBM-9 041119	
Information Exposure	29-10-2019	5	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores sensitive information in cleartext within a resource that might be accessible to another control sphere. IBM X-Force ID: 1610141. CVE ID: CVE-2019-4314			https://ibm.com port/pag ode/109	/sup ges/n	A-IBM-9 041119		
Improper Input Validation	29-10-2019	4	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 161209. CVE ID: CVE-2019-4329		https://www. ibm.com/sup port/pages/n ode/1096906		A-IBM-SECU- 041119/265			
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
Reliance on Cookies without Validation and Integrity Checking	29-10-2019	4.3	(Sona the se cooki which agent cooki an H7	Big Data Intelligence (SonarG) 4.0 does not set the secure attribute for cookies in HTTPS sessions, which could cause the user agent to send those cookies in plaintext over an HTTP session. IBM X-Force ID: 161210. CVE ID: CVE-2019-4330				www. i/sup ges/n 96384	A-IBM-S 041119	
Inadequate Encryption Strength	29-10-2019	5	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses weaker than expected cryptographic algorithms that could allow an				https:// ibm.com port/pag ode/109	ı/sup ges/n	A-IBM-S 041119	
cloud_orches	trator									
Improper Input Validation	25-10-2019	2.1	2.4 th throu APIs to a loca	APIs that could be used by a local user to send email. IBM X-Force ID: 162232.		https://www. ibm.com/sup port/pages/n ode/1097301		A-IBM-0 041119		
Information Exposure	25-10-2019	2.1	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a local user to obtain sensitive information from temporary script files. IBM X-Force ID: 162333. CVE ID: CVE-2019-4395			https://www. ibm.com/sup port/pages/n ode/1097175		A-IBM-0 041119		
Improper	25-10-2019	3.5	IBM (Cloud Or	chestrat	or	https://	www.	A-IBM-0	CLOU-
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	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')			through 2.5.0.9 is vulnerable to HTTP response splitting attacks, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject arbitrary HTTP headers and cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning or cross-site scripting, and possibly obtain sensitive information. IBM X-Force ID: 162236. CVE ID: CVE-2019-4396 IBM Cloud Orchestrator				ibm.com port/pag ode/109	ges/n	041119	/270
Information Exposure	24-10-2019	4	and II Orche 2.5 th throu sensit URL I lead t disclo partic URLs refer brow Force	and IBM Cloud Orchestrator Enterprise 2.5 through 2.5.0.9 and 2.4 through 2.4.0.5 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X- Force ID: 162239 CVE ID: CVE-2019-4397		https://ibm.com port/pag ode/107	/sup ges/n 7147	A-IBM-0 041119		
Missing Encryption of Sensitive	24-10-2019	2.1	and I	IBM Cloud Orchestrator and IBM Cloud Orchestrator Enterprise			https://ibm.com port/pag	/sup	A-IBM-0 041119	
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
Data			2.5 through 2.5.0.9 and 2.4 through 2.4.0.5 could allow a local user to obtain sensitive information from SessionManagement cookies. IBM X-Force ID: 162259. CVE ID: CVE-2019-4398	ode/1077123	
Use of a Broken or Risky Cryptograph ic Algorithm	25-10-2019	5	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 162260. CVE ID: CVE-2019-4399	https://www. ibm.com/sup port/pages/n ode/1097307	A-IBM-CLOU- 041119/273
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-10-2019	4	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 162261. CVE ID: CVE-2019-4400	https://www. ibm.com/sup port/pages/n ode/1077129	A-IBM-CLOU- 041119/274
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	3.5	IBM Cloud Orchestrator and IBM Cloud Orchestrator Enterprise 2.5 through 2.5.0.9 and 2.4 through 2.4.0.5 is vulnerable to cross-site scripting. This vulnerability allows users	https://www. ibm.com/sup port/pages/n ode/1096342	A-IBM-CLOU- 041119/275

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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: 163656.		
			CVE ID : CVE-2019-4459		
Improper Input Validation	25-10-2019	3.5	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 is vulnerable to HTTP Response Splitting caused by improper caching of content. This would allow the attacker to perform further attacks, such as Web Cache poisoning, cross-site scripting and possibly obtain sensitive information. IBM X-Force ID: 163682. CVE ID: CVE-2019-4461	https://www. ibm.com/sup port/pages/n ode/1072684	A-IBM-CLOU- 041119/276
cloud_orches	strator_enterp	rise			
Information Exposure	24-10-2019	4	IBM Cloud Orchestrator and IBM Cloud Orchestrator Enterprise 2.5 through 2.5.0.9 and 2.4 through 2.4.0.5 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 162239	https://www. ibm.com/sup port/pages/n ode/1077147	A-IBM-CLOU- 041119/277

4-5

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
			CVE I	D : CVE-	2019-4	397				
Missing Encryption of Sensitive Data	24-10-2019	2.1	and II Orche 2.5 th throu allow sensit Sessic cooki 1622	allow a local user to obtain sensitive information from SessionManagement cookies. IBM X-Force ID: 162259. CVE ID: CVE-2019-4398			https://ibm.com port/pag ode/107	/sup ges/n	A-IBM-(041119	
db2_high_per	rformance_un	load_lo	ad							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-10-2019	7.2	Perfo for LU vulne overf impro which attack arbiti syste privil	IBM DB2 High Performance Unload load for LUW 6.1 and 6.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 165481.		https://suppo rtcontent.ibm. com/support/ pages/node/1 073236		A-IBM-I 041119		
maximo_heal	lth_safety_a	ıd_envi	ironme	ent_man	ager					
Improper Privilege Managemen t	29-10-2019	6.5	After installing the IBM Maximo Health- Safety and Environment Manager 7.6.1, a user is granted additional privileges that they are not normally allowed to access. IBM X- Force ID: 165948. CVE ID: CVE-2019-4546		https://www. ibm.com/sup port/pages/n ode/1087738		A-IBM-N 041119			
api_connect										
Information	29-10-2019	5	IBM A	API Conn	ect vers	ion	https://www.		A-IBM-API	
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
Exposure			V5.0.0.0 through 5.0.8.7 could reveal sensitive information to an attacker using a specially crafted HTTP request. IBM X-Force ID: 167883.	ibm.com/sup port/pages/n ode/1079127	041119/281
maximo_asse	et_managemen	t			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 164070. CVE ID: CVE-2019-4486	https://www.ibm.com/support/pages/node/1075023	A-IBM-MAXI- 041119/282
maximo_for_	aviation				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 164070.	https://www. ibm.com/sup port/pages/n ode/1075023	A-IBM-MAXI- 041119/283
			CVE ID : CVE-2019-4486		

Weakness	Pu	blish Date	e CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	PC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-	10-2019	3.5	Mana vulne script vulne to em JavaS UI thu intendence crede withi	Maximo agement brable to ting. This brability abed arbust alterioded functially lead that alteriols dientials dienti	7.6 is cross-sis allows ustrary de in the etionality ading to sclosure ed sessi	sers Web y e on. 70.	https:// ibm.com port/pag ode/107	ı/sup ges/n	A-IBM-l 041119	
maximo_for_	nucl	ear_pov	ver	CVE ID : CVE-2019-4486 IBM Maximo Asset							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-	10-2019	3.5	Mana vulne script vulne to em JavaS UI thu inten- poten crede withi	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 164070.			https:// ibm.com port/pag ode/107	l/sup ges/n	A-IBM-l 041119	
maximo_for_	oil_a	nd_gas									
Improper Privilege Managemen t	29-	10-2019	6.5	After installing the IBM Maximo Health- Safety and Environment Manager 7.6.1, a user is granted additional privileges that they are not normally allowed to access. IBM X- Force ID: 165948. CVE ID: CVE-2019-4546			https:// ibm.com port/pag ode/108	ı/sup ges/n	A-IBM-I 041119		
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 164070. CVE ID: CVE-2019-4486	https://www.ibm.com/support/pages/node/1075023	A-IBM-MAXI- 041119/287
maximo_for_	transportation	1			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 164070. CVE ID: CVE-2019-4486	https://www. ibm.com/sup port/pages/n ode/1075023	A-IBM-MAXI- 041119/288
maximo_for_	utilities				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	3.5	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	https://www. ibm.com/sup port/pages/n ode/1075023	A-IBM-MAXI- 041119/289
CV Scoring Sca (CVSS)	o-1	1-2	2-3 3-4 4-5 5-6 110	6-7 7-8	8-9 9-10

Weakness	Pub	lish Date	CVSS	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
				crede withi	itially lea ntials di n a trust K-Force I	sclosure ed sessi	on.				
				CVE I	D : CVE-	2019-4	486				
smartcloud_c	contro	ol_desk									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-1	0-2019	3.5	Mana vulne script vulne to em JavaS UI thu intende potent crede within	Maximo Agement rable to rability ability ability ability ability ability alterinded functially lead functially lead atrust ability abi	7.6 is cross-si s allows ustrary de in the stionality ading to sclosure ed session	sers Web	https:// ibm.com port/pag ode/107	/sup ges/n	A-IBM-S 041119	
				CVE I	D : CVE-	2019-4	486				
tivoli_integra	ation_	compo	ser								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-1	0-2019	3.5	JavaScript code in the Web UI thus altering the		https:// ibm.com port/pag ode/107	/sup ges/n	A-IBM-7 041119			
tivoli_worklo	oad_so	chedule	er								
Improper Privilege	16-1	0-2019	7.2		Vorkload buted 9.			https:// ibm.com		A-IBM-7 041119	
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Managemen t			vulne allow files a system the at privil 1559	.5 conta rability a local us ns root ir m, which ctacker to eges. IBI 97.	that cou user to v the file o could a o gain ro M X-Fore	vrite allow oot ce ID:	port/pag ode/107	-		
security_acce	ess_manager									
Improper Input Validation	25-10-2019	5	Mana allow attacl of ser proxy Force	Gecurity ger App to unauthouser to carrice in to compose ID: 156	liance co enticate use a de he rever nent. IBI 159.	d nial rse M X-	https://ibm.com port/pag ode/107	A-IBM-9 041119		
ics										
kea										
Reachable Assertion	16-10-2019	3.3	A packet containing a malformed DUID can cause the Kea DHCPv6 server process (keadhcp6) to exit due to an assertion failure. Versions affected: 1.4.0 to 1.5.0, 1.6.0-beta1, and 1.6.0-beta2. CVE ID: CVE-2019-6472				https:// org/doc 2019-64	s/cve-	A-ICS-K 041119	
Reachable Assertion	16-10-2019	3.3	An invalid hostname option can trigger an assertion failure in the Kea DHCPv4 server process (kea-dhcp4), causing the server process to exit. Versions affected: 1.4.0 to 1.5.0, 1.6.0-beta1, and				https:/// org/doc 2019-64	s/cve-	A-ICS-K 041119	
CV Scoring Sca	lle 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			1.6.0-	beta2.						
			CVE I	D : CVE-	2019-6	473				
Igniterealtim	ie									
openfire										
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-10-2019	5	Realti 4.4.2 retrie under direct trave	nServlet ime Ope does not eved files tory, aka rsal vuln D: CVE-	nfire thr ensure are loca enfire ho a direct erability	that ated ome cory	N/A		A-IGN-0 041119	
Server-Side Request Forgery (SSRF)	24-10-2019	7.5	18393 A Server Side Request Forgery (SSRF) vulnerability in FaviconServlet.java in Ignite Realtime Openfire through 4.4.2 allows attackers to send arbitrary HTTP GET requests. CVE ID: CVE-2019- 18394				N/A		A-IGN-0 041119	
ISC										
kea										
Improper Input Validation	16-10-2019	6.1	A missing check on incoming client requests can be exploited to cause a situation where the Kea server's lease storage contains leases which are rejected as invalid when the server tries to load leases from storage on restart. If the number of such leases exceeds a hard-coded limit in the Kea code, a server trying				https:// org/doc 2019-64	s/cve-	A-ISC-K 041119	
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
			to restart will conclude that there is a problem with its lease store and give up. Versions affected: 1.4.0 to 1.5.0, 1.6.0-beta1, and 1.6.0-beta2 CVE ID: CVE-2019-6474		
bind	<u>'</u>			<u> </u>	<u> </u>
Improper Input Validation	17-10-2019	5	Mirror zones are a BIND feature allowing recursive servers to pre-cache zone data provided by other servers. A mirror zone is similar to a zone of type secondary, except that its data is subject to DNSSEC validation before being used in answers, as if it had been looked up via traditional recursion, and when mirror zone data cannot be validated, BIND falls back to using traditional recursion instead of the mirror zone. However, an error in the validity checks for the incoming zone data can allow an on-path attacker to replace zone data that was validated with a configured trust anchor with forged data of the attacker's choosing. The mirror zone feature is most often used to serve a local copy of the root zone. If an attacker was able to insert themselves into the network path between a	https://kb.isc. org/docs/cve- 2019-6475, https://securi ty.netapp.com /advisory/nta p-20191024- 0004/	A-ISC-BIND- 041119/299

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			mirro name vulne used recur a cop zone BIND 9.14.6		this could th the ver to ac fied roo is affects s 9.14.0	en be cept t s up to				
Reachable Assertion	17-10-2019	5	suppo minir name asser forwa referr resolv affect 9.14.0	named to exit with an assertion failure if a forwarder returns a referral rather than resolving the query. This affects BIND versions p-2			https://org/doc. 2019-64 https://s ty.netap /advisor p-20191 0004/	s/cve- 76, securi p.com	A-ISC-B 041119	
Jenkins										
bumblebee_h	ıp_alm									
Improper Certificate Validation	16-10-2019	6.4	ALM earlie disab hostn	ns Bumb Plugin 4 er uncon led SSL/ name ver ections t D : CVE	.1.3 and ditional TLS and rification o HP AL	ly l ı for	https://jenkin s.io/security/ advisory/201 r 9-10- 16/#SECURIT Y-1481		A-JEN-E 041119	
google_kube	rnetes_engin	e								
Incorrect Permission Assignment	16-10-2019	4	A missing permission https://jenkocheck in Jenkins Google s.io/security advisory/20			ırity/	A-JEN-0 041119			
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3-4	4-5	4-5 5-6 6-7			8-9	9-10

Weakness	Pu	blish Date	e CVS	S D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
for Critical Resource				attack Overa to ob inform scope an attack	and earlesters with lall/Read tain limi mation are of a creacker-spentials II (D:CVE)	n permiss ted bout the dential pecified).	sion e	9-10- 16/#SE0 Y-1607	CURIT		
cadence_vma	nag	er									
Improper Certificate Validation	16-	10-2019	6.4	Plugi disab hostr globa maste	ns Cader n 2.7.0 a led SSL/ name ver llly for ther JVM. ID: CVE	nd earli TLS and rification ne Jenkir	er I	https:// s.io/secu advisory 9-10- 16/#SE0 Y-1615	rity/ //201	A-JEN-0 041119	
oracle_cloud	_infr	astructi	ure_con	npute_c	lassic						
Cross-Site Request Forgery (CSRF)	16-	10-2019	4.3	forge Jenki Infras Class attack attack using crede	A cross-site request forgery vulnerability in Jenkins Oracle Cloud Infrastructure Compute Classic Plugin allows attackers to connect to an attacker-specified URL https:// s.io/sec advisory 9-10-			16/#SE0	rity/ v/201	A-JEN-0 041119	
				1045	D : CVE	-2019-					
Incorrect Permission Assignment for Critical Resource	16-	10-2019	4	check Cloud Comp allow Overa to con	A missing permission check in Jenkins Oracle Cloud Infrastructure Compute Classic Plugin allows attackers with Overall/Read permission to connect to an attackerspecified URL using			https:/// s.io/secu advisory 9-10- 16/#SE0 Y-1462	rity/ //201	A-JEN-0 041119	
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	3-4	4-5	4-5 5-6 6-7			8-9	9-10

Weakness	Pub	lish Date	CVSS	D	escription	n & CVE I	D	Pato	h	NCIIP	C ID
				crede	xer-spec ntials. D : CVE-						
				1045	7						
deploy_weble	ogic										
Cross-Site Request Forgery (CSRF)	23-1	10-2019	6.8	forger Jenkir Plugir conne specif attack crede wheth with a path o	-	rability y WebLe attacked using ified or director director the Jenlestem.	ogic rs to r- nine ctory ified	https://j s.io/secu advisory 9-10- 23/#SE0 Y-820	rity/ 7/201	A-JEN-D 041119	
				CVE ID : CVE-2019- 10464							
Incorrect Default Permissions	23-1	10-2019	4	A missing permission check in Jenkins Deploy WebLogic Plugin allows attackers with Overall/Read permission to connect to an attackerspecified URL using attacker-specified credentials, or determine whether a file or directory		https://j s.io/sect advisory 9-10- 23/#SE0 Y-820	rity/ //201	A-JEN-E 041119			
				1046	5						
soasta_cloud	test			Ignlein	ne SOAS'	ΓΔ Claus	dTact	https://	ionkin		
Cleartext Storage of Sensitive	16-1	10-2019	4	Jenkins SOASTA CloudTest Plugin stores credentials unencrypted in its global configuration file on the		s.io/sed bal advisor		irity/	A-JEN-S 041119		
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
Information			Jenkins master where they can be viewed by users with access to the master file system. CVE ID: CVE-2019-	16/#SECURIT Y-1439	
aofy ai			10451		
sofy.ai			Jenkins Sofy.AI Plugin		
Cleartext Storage of Sensitive Information	16-10-2019	4	stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. CVE ID: CVE-2019- 10447	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1431	A-JEN-SOFY- 041119/309
extensive_tes	sting				
Insufficientl y Protected Credentials	16-10-2019	4	Jenkins Extensive Testing Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. CVE ID: CVE-2019- 10448	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1432	A-JEN-EXTE- 041119/310
fortify_on_de	mand				
Cleartext Storage of Sensitive Information	16-10-2019	4	Jenkins Fortify on Demand Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1433	A-JEN-FORT- 041119/311
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	Pub	lish Date	cvss	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
				_		r access e system					
				CVE I 1044	D : CVE	-2019-					
elasticbox_ci											
Cleartext Storage of Sensitive Information	16-1	10-2019	2.1	unend config file on where by use maste CVE I	Plugin stores credentials unencrypted in the global config.xml configuration file on the Jenkins master where they can be viewed by users with access to the master file system. CVE ID: CVE-2019- 10450 Jenkins View26 Test- Reporting Plugin stores credentials unencrypted in job config.xml files on the		urity/ v/201	A-JEN-E 041119			
view26_test-	repoi	rting									
Cleartext Storage of Sensitive Information	Storage of Sensitive 16-10-2019		4	Report crede job co Jenkin can be with left perm the m	rting Pluntials under the configron of t	ngin stor nencrypt I files on er where d by usen d Read r access e system	ted in the they extra to	https://j s.io/sect advisory 9-10- 16/#SEC Y-1440	urity/ v/201	A-JEN-V 041119	
				1045		2017					
puppet_enter	pris	e_pipelii	1e								
Improper Input Validation	16-1	10-2019	6.5	Jenkins Puppet Enterprise Pipeline 1.3.1 and earlier specifies unsafe values in its custom Script Security whitelist, allowing attackers able to execute Script Security protected scripts to execute arbitrary code. CVE ID: CVE-2019-		https://j s.io/sect advisory 9-10- 16/#SE0 Y-918	urity/ v/201	A-JEN-F 041119			
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
			1045	8						
bitbucket_oa	uth									
Insufficientl y Protected Credentials	23-10-2019	Plugin 0.9 and earlier stored credentials unencrypted in the global config.xml configuration file on the Jenkins master where they could be viewed by users with access to the master file system. CVE ID: CVE-2019-10460				stored credentials unencrypted in the global config.xml configuration file on the Jenkins master where they could be viewed by users with access to the master file system. CVE ID: CVE-2019- 10460 A cross-site request forgery vulnerability in Jenkins Libvirt Slaves Plugin allows attackers to connect to an attacker- specified SSH server using attacker-specified				BITB- /315
libvirt_slaves	3									
Cross-Site Request Forgery (CSRF)	23-10-2019	6.8	forge: Jenkir Plugir conne specif attack crede throu captu store CVE I	A cross-site request forgery vulnerability in Jenkins Libvirt Slaves Plugin allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. CVE ID: CVE-2019-				jenkin urity/ v/201 CURIT	A-JEN-L 041119	
Incorrect Default Permissions	23-10-2019	4	stored in Jenkins.			https://j s.io/secu advisory 9-10- 23/#SEC Y- 1014%2	urity/ v/201 CURIT	A-JEN-L 041119		
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish [Date	CVSS	D	escription	a & CVE I	D	Pato	:h	NCIIP	CID
					d in Jenk D : CVE- 2						
Incorrect Default Permissions	23-10-20	019	4	check Slaves relate users acces crede crede Jenkin	D : CVE-	ns Libvi in form- ds allov erall/Re nerate of ored in	rt ved	https://s.io/sect advisory 9-10- 23/#SE6 Y- 1014%2	urity/ v/201 CURIT	A-JEN-L 041119	
global_post_s	cript			A missing permission							
Incorrect Default Permissions	23-10-20	019	4	check Post S allow Overa the so plugin Jenkin	in Jenki Script Plused users all/Read cripts ava n stored ns maste D: CVE-	ns Globa ugin in with access t ailable to on the r file sys	al o list o the	https://s.io/sectadvisory 9-10- 23/#SE0 Y-1073	urity/ v/201	A-JEN-0 041119	
google_oauth	_credent	ials									
Information Exposure	16-10-20	019	4	An arbitrary file read vulnerability in Jenkins Google OAuth Credentials Plugin 0.9 and earlier allowed attackers able to configure jobs and credentials in Jenkins to obtain the contents of any file on the Jenkins master. CVE ID: CVE-2019-10436				https://s.io/secuadvisory 9-10- 16/#SE0 Y-1583	urity/ v/201	A-JEN-0 041119	
crx_content_j	package_	deplo	yer								
CV Scoring Sca (CVSS)	le 0 -1	1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	forge: Jenkir Packa 1.8.1 attack attack using crede throu captu storee	ss-site rory vulne ns CRX Cage Depland earl sers to caster-specattacker ntials ID gh anothering cred in Jenk d in Jenk D: CVE-	rability content coyer Plu ier allov connect t ified UR r-specifi s obtair ner metl dentials cins.	gin ved o an L ed ied nod,	https://j s.io/secu advisory 9-10- 16/#SE0 Y- 1006%2	urity/ v/201 CURIT	A-JEN-0 041119	
Incorrect Permission Assignment for Critical Resource	16-10-2019	4	check Conte Plugin allow Overa to con specifi attack crede throu captu stored		ns CRX age Depl nd earlickers wit permiss an attact using ified os obtain ner metl dentials tins.	loyer er h sion ker- led nod,	https://j s.io/secu advisory 9-10- 16/#SE0 Y- 1006%2	rity/ 7/201 CURIT	A-JEN-0 041119	
Insufficientl y Protected Credentials	16-10-2019	4	CVE ID: CVE-2019- 10438 A missing permission check in Jenkins CRX Content Package Deployer Plugin 1.8.1 and earlier in various 'doFillCredentialsIdItems' methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.				https://j s.io/sect advisory 9-10- 16/#SEC Y- 1006%2	urity/ c/201 CURIT	A-JEN-0 041119	_
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
			CVE ID : CVE-2019- 10439		
neoload					
Cleartext Storage of Sensitive Information	16-10-2019	4	Jenkins NeoLoad Plugin 2.2.5 and earlier stored credentials unencrypted in its global configuration file and in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system.	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1427	A-JEN-NEOL- 041119/324
			CVE ID : CVE-2019- 10440		
icescrum					
Cross-Site Request Forgery (CSRF)	16-10-2019	4.3	A cross-site request forgery vulnerability in Jenkins iceScrum Plugin 1.1.5 and earlier allowed attackers to connect to an attacker-specified URL using attacker-specified credentials. CVE ID: CVE-2019-	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1484	A-JEN-ICES- 041119/325
			10441		
Incorrect Permission Assignment for Critical Resource	16-10-2019	4	A missing permission check in Jenkins iceScrum Plugin 1.1.5 and earlier allowed attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials. CVE ID: CVE-2019-	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1484	A-JEN-ICES- 041119/326
			10442		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	16-10-2019	4	Jenkins iceScrum Plugin 1.1.4 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system. CVE ID: CVE-2019- 10443	https://jenkin	A-JEN-ICES- 041119/327
delphix	<u> </u>				
Cleartext Storage of Sensitive Information	16-10-2019	2.1	Jenkins Delphix Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. CVE ID: CVE-2019-10453	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1450	A-JEN-DELP- 041119/328
rundeck					
Cross-Site Request Forgery (CSRF)	16-10-2019	4.3	A cross-site request forgery vulnerability in Jenkins Rundeck Plugin allows attackers to connect to an attacker-specified URL using attacker-specified credentials. CVE ID: CVE-2019-10454	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT Y-1460	A-JEN-RUND- 041119/329
Incorrect Permission Assignment for Critical Resource	16-10-2019	4	A missing permission check in Jenkins Rundeck Plugin allows attackers with Overall/Read permission to connect to an attacker-specified URL	https://jenkin s.io/security/ advisory/201 9-10- 16/#SECURIT	A-JEN-RUND- 041119/330
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			_	attackeı ntials.	r-specifi	ed	Y-1460			
			CVE I 1045	D : CVE- 5	2019-					
mattermost_	notification									
Insufficientl y Protected Credentials	23-10-2019	4	Jenkins Dynatrace				https://j s.io/secu advisory 9-10- 23/#SE0 Y-1628	rity/ /201	A-JEN-N 041119	
	1	., .		9						
dynatrace_ap	oplication_m	onitorin	•	Р .						
Insufficientl y Protected Credentials	23-10-2019	2.1	Jenkins Dynatrace Application Monitoring Plugin 2.1.3 and earlier stored credentials unencrypted in its global configuration file on the			https://j s.io/secu advisory 9-10- 23/#SE0 Y-1477	rity/ /201	A-JEN-D 041119		
			1046	D : CVE- 1	4U17					
Cross-Site Request Forgery (CSRF)	23-10-2019	6.8	A cross-site request forgery vulnerability in Jenkins Dynatrace Application Monitoring Plugin 2.1.3 and earlier allowed attackers to			https://jenkin s.io/security/ advisory/201 9-10- 23/#SECURIT Y-		A-JEN-DYNA- 041119/333		
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	Pul	olish Date	cvss	S Description & CVE ID				Pato	h	NCIIP	C ID
				specif attacl	ect to an fied URL ker-spec ntials.	using	r-	1483%2	0(1)		
				CVE I 1046	D : CVE- 2	2019-					
Incorrect Default Permissions	23-	10-2019	4	A missing permission check in Jenkins Dynatrace Application Monitoring Plugin allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials. CVE ID: CVE-2019-10463				https://j s.io/sect advisory 9-10- 23/#SEC Y- 1483%2	rity/ /201 CURIT	A-JEN-D 041119	
				CVE ID : CVE-2019-							
360_fireline											
Improper Restriction of XML External Entity Reference ('XXE')	23-	10-2019	5.5	(XXE) Jenkin Plugin with (to have extern in the from serve forge service	An XML external entities (XXE) vulnerability in Jenkins 360 FireLine Plugin allows attackers with Overall/Read access to have Jenkins resolve external entities, resulting in the extraction of secrets from the Jenkins agent, server-side request forgery, or denial-of- service attacks. CVE ID: CVE-2019-				enkin arity/ c/201 CURIT	A-JEN-3 041119	
sonar_gerrit											
Insufficientl y Protected Credentials	23-	10-2019	4	Jenkins Sonar Gerrit Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users				https://jenkin s.io/security/ advisory/201 9-10- 23/#SECURIT		A-JEN-S 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			perm	Extended ission, o aster filo	r access		Y-1003			
			CVE I 1046	D : CVE- 7	2019-					
kubernetes_c	ci									
Cross-Site Request Forgery (CSRF)	23-10-2019	6.8	forge Jenkin Kube allow conne specin attacl crede throu captu store	ss-site re ry vulne ns Elasti- rnetes C s attacke ect to an fied URL ker-spec entials ID gh anoth ring cre- d in Jenk	rability: cBox Jer I/CD Pluers to attacker using ified is obtain ner meth dentials ins.	nkins ngin r- ned nod,	https://j s.io/secu advisory 9-10- 23/#SE0 Y- 1005%2	urity/ v/201 CURIT	A-JEN-k 041119	
					2019-					
Incorrect Default Permissions	23-10-2019	4	CVE ID: CVE-2019- 10468 A missing permission check in Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.				https://j s.io/sect advisory 9-10- 23/#SEC Y- 1005%2	urity/ v/201 CURIT	A-JEN-k 041119	
			CVE ID : CVE-2019- 10469							
Incorrect Default Permissions	23-10-2019	4	A missing permission check in Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin			https://jenkin s.io/security/ advisory/201 gin 9-10-		A-JEN-k 041119		
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	e CVSS	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			allow Overa enum of cre Jenkin	D : CVE-	with access t edential stored i	o s ID	23/#SE0 Y- 1005%2			
build-metric	S									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	script Jenkin Plugin inject JavaSe provi	ected croing vulnus build- nallows arbitrar cript into ded by the D: CVE- 5	erability metrics attacker by HTML o web pa his plugi	rs to and ages	https://j s.io/sect advisory 9-10- 23/#SEC Y-1490	rity/ //201	A-JEN-E 041119	
zulip										
Insufficientl y Protected Credentials	23-10-2019	2.1	Jenkins Zulip Plugin 1.1.0 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file				https:// s.io/sect advisory 9-10- 23/#SE0 Y-1621	rity/ /201	A-JEN-Z 041119	
K7computing	3									
k7_antivirus	premium									
Improper Privilege Managemen t	28-10-2019	7.5	In K7 Antivirus Premium 16.0.xxx through 16.0.0120; K7 Total Security 16.0.xxx through 16.0.0120; and K7 Ultimate Security 16.0.xxx				N/A		A-K7C-I 041119	
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
			through 16.0.0120, the module K7TSHlpr.dll improperly validates the administrative privileges of the user, allowing arbitrary registry writes in the K7AVOptn.dll module to facilitate escalation of privileges via interprocess communication with a service process. CVE ID: CVE-2019-16897		
k7_total_secu	irity				
Improper Privilege Managemen t	28-10-2019	7.5	In K7 Antivirus Premium 16.0.xxx through 16.0.0120; K7 Total Security 16.0.xxx through 16.0.0120; and K7 Ultimate Security 16.0.xxx through 16.0.0120, the module K7TSHlpr.dll improperly validates the administrative privileges of the user, allowing arbitrary registry writes in the K7AVOptn.dll module to facilitate escalation of privileges via inter- process communication with a service process. CVE ID: CVE-2019- 16897	N/A	A-K7C-K7_T- 041119/343
k7_ultimate_	security				
Improper Privilege Managemen t	28-10-2019	7.5	In K7 Antivirus Premium 16.0.xxx through 16.0.0120; K7 Total Security 16.0.xxx through 16.0.0120; and K7	N/A	A-K7C-K7_U- 041119/344
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				Pato	h	NCIIP	C ID
			throu modu impro admin of the arbitr the K' to fac privil proce with a	ate Secu gh 16.0.1 le K7TS operly vanistrative user, all ary reginary reginary 7AVOptralitate es eges via ess commans service D: CVE-	0120, the Hlpr.dll alidates to privile lowing stry write alation internunication process	che ges tes in dule of				
Kubernetes			1007	, 						
kubernetes										
Improper Input Validation	17-10-2019	5	in the serve 1.12 a v1.13 and v author malic paylo serve exces poten become Prior RBAC anony submatrigge Cluster version in the serve i	oper inportance in version versions YAM ads, causer to constict to v1.14 policy a po	etes API ions v1.0 ions prio 4.8, v1.1 lows ers to se ML or JSO sing the sume or men ashing a available uthorize sers to sts that o linerabil aded fro to v1.14	or to .5.5, end ON API nory, nd llt ed could ity. m a	https://s b.com/k etes/kul es/issue 53	ubern ernet	A-KUB-1 041119	
			backv	by defa vards co D : CVE-	ult for mpatibil	lity.				

Weakness	Pu	blish Date	cvss	D	escriptio	n & CVE I	D		Pato	:h	NCIIF	CID
				1125	3							
Libarchive				<u> </u>				<u>. </u>				
libarchive												
Use After Free	24-	10-2019	5	archive_read_format_rar_r ead_data in archive_read_support_for mat_rar.c in libarchive before 3.4.0 has a use- after-free in a certain ARCHIVE_FAILED situation, related to Ppmd7_DecodeSymbol. CVE ID : CVE-2019- 18408 A heap buffer overflow bug in				N/A			A-LIB-L 041119	
libpl_droidso	nro	ids_gif_p	roject					<u> </u>				
libpl_droidso	nro	ids_gif										
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-	10-2019	7.5	bug in libpl_ befor What befor could attack arbitr denia	bug in libpl_droidsonroids_gif before 1.2.19, as used in WhatsApp for Android before version 2.19.291 could allow remote attackers to execute arbitrary code or cause a denial of service. CVE ID: CVE-2019-				attps://acebool security sories/0 2019-11	cve-	A-LIB-L 041119	
libpod_proje	ct			•								
libpod												
Improper Link Resolution Before File Access ('Link Following')	28-	10-2019	5.8	An issue was discovered in Podman in libpod before 1.6.0. It resolves a symlink in the host context during a copy operation from the container to the host, because an undesired glob operation occurs. An				N	N/A		A-LIB-L 041119	
CV Scoring Sca (CVSS)	ile	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	D	Description & CVE ID				atch	NCIIP	PC ID
			container image containing particular symlinks that, when copied by a victim user to the host filesystem, may overwrite existing files with others from the host. CVE ID: CVE-2019- 18466							
11 10			18466							
Libssh2										
libssh2			7 1.1	ssh2 v1.9	20 1				 	
Integer Overflow or Wraparoun d	21-10-2019	5.8	earlie SSH_N logic i intege bound attack arbitr offset memo SSH s disclo inform denia on the a user serve	r version MSG_DIS in packet er overfleds check ker to specification for a subserver mander erver mation of service clients connected. D: CVE-	ns, the CONNEO t.c has a ow in a enablir ecify an ecify and be about tive reause a fice cond ystem was to the	ng an nds) at ed le to a ition when	N/A		A-LIB-L 041119	
Limesurvey limesurvey										
Improper Neutralizati on of Input During Web Page Generation	16-10-2019	9 4.3	A cross-site scripting (XSS) vulnerability in admin/translate/translate header_view.php in LimeSurvey 3.19.1 and earlier allows remote				N/A		A-LIM-I 041119	
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			D	Pato	h	NCIIP	C ID
('Cross-site Scripting')			arbitr HTMI paran demo index e/sa/	xers to in cary web via the neter, as nstrated php/ad index/si ang/ PA	script of tolang I by the min/tra urveyid,	nslat /336				
			CVE I 1766	D : CVE- 0	2019-					
loofah_proje	ct		<u> </u>							
loofah										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	22-10-2019	3.5	Ruby unsar may o outpu eleme	Loofah through nitized Ja occur in s et when a ent is rep D : CVE- 7	v2.3.0 avaScrip sanitized a crafted publishe	t d l SVG	https://s b.com/fl ones/loo ssues/17	avorj ofah/i	A-L00-l 041119	
managewp										
broken_link_	checker									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	plugin Word Link (susce XSS d encod an HT into H functi listing links provi in the paran filter_	roken-ling through Press (an Checker) ptible to implie to implie to implie the total through the terminal through the terminal through the terminal through th	h 1.11.8 ka Brok is Reflecte proper insertio parame ne filter te page ected bro xploited XSS payl GET a ch reque	for en ed on of ter oken by load	N/A		A-MAN- BROK- 041119	
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	n & CVE ID		Pato	:h	NCIIP	C ID
			product. CVE ID : CVE- 16521	-2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	18-10-2019	3.5	A reflected XSS vulnerability was found in includes/admin/table- printer.php in the broken- link-checker (aka Broken Link Checker) plugin 1.11.8 for WordPress. This allows unauthorized users to inject client-side JavaScript into an admin- only WordPress page via the wp- admin/tools.php?page=vie w-broken-links s_filter parameter in a search action. CVE ID: CVE-2019- 17207		N/A		A-MAN- BROK- 041119		
mapr									
mapr									
Improper Input Validation	24-10-2019	7.5	vulnerability MapR CLDB c specifically in framework th the CLDB cod handles login issuance. An a use the 'class' the JSON requ the CLDB to in JSON library's which Java cla request is des	A remote code execution vulnerability exists in MapR CLDB code, specifically in the JSON framework that is used in the CLDB code that handles login and ticket issuance. An attacker can use the 'class' property of the JSON request sent to the CLDB to influence the JSON library's decision on which Java class this JSON request is deserialized to. By doing so, the attacker				A-MAP- MAPR- 041119	
CV Scoring Sca	le 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
			to construct a URLClassLoader which loads a malicious Java class from a remote path and instantiate this object in the MapR CLDB, thus executing arbitrary code on the machine running the MapR CLDB and take over the cluster. By switching to the newer Jackson library and ensuring that all incoming JSON requests are only deserialized to the same class that it was serialized from, the vulnerability is fixed. This vulnerability affects the entire MapR core platform. CVE ID: CVE-2019- 12017		
Metinfo					
metinfo					
Cross-Site Request Forgery (CSRF)	17-10-2019	6.8	app/system/admin/admin/index.class.php in MetInfo 7.0.0beta allows a CSRF attack to add a user account via a doSaveSetup action to admin/index.php, as demonstrated by an admin/?n=admin&c=index &a=doSaveSetup URI. CVE ID: CVE-2019-	N/A	A-MET-METI- 041119/355
Mi av - C-			17676		
Microfocus	rvico nasswer	d rose	•		
neuq_sen_se	rvice_passwor	u_rese	l .		

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	1-2	7	†) †	3-0	0-7	7	5	J-10

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D		Pato	h	NCIIP	C ID	
Improper Certificate Validation	22-10-2019	4.3	Focus Passv all ve 4.4.0. could certif may r the-m	vulnerability in Micro Focus Self Service Password Reset, affecting all versions prior to 4.4.0.4. The vulnerability could exploit invalid certificate validation and may result in a man-in- the-middle attack. CVE ID: CVE-2019- 11674						A-MIC-NETI- 041119/356		
			11674									
mindpalette												
natemail												
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	Script vulne Mind 3.0.15 to exe JavaS brow crafte application the array is key defau will b	A reflected Cross-Site Scripting (XSS) vulnerability in MindPalette NateMail 3.0.15 allows an attacker to execute remote JavaScript in a victim's browser via a specially crafted POST request. The application will reflect the recipient value if it is not in the NateMail recipient array. Note that this array is keyed via integers by default, so any string input will be invalid. CVE ID: CVE-2019-				/A		A-MIN-1 041119		
mp3gain_pro	oject											
mp3gain												
Improper Restriction of Operations within the	23-10-2019	4.3	A buffer over-read was discovered in ReadMP3APETag in apetag.c in MP3Gain 1.6.2. The vulnerability causes				N,	/A		A-MP3- 041119		
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
Bounds of a Memory Buffer			an application crash, which leads to remote denial of service. CVE ID: CVE-2019-		
			18359		
Mulesoft					
mule_runtim	ie			T	
Deserializati on of Untrusted Data	16-10-2019	7.5	The MuleSoft Mule Community Edition runtime engine before 3.8 allows remote attackers to execute arbitrary code because of Java Deserialization, related to Apache Commons Collections	N/A	A-MUL- MULE- 041119/359
			CVE ID: CVE-2019- 13116		
Nchsoftware					
express_acco	unts_accounti	ng		,	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	3.5	In NCH Express Accounts Accounting v7.02, persistent cross site scripting (XSS) exists in Invoices/Sales Orders/Items/Customers/ Quotes input field. An authenticated unprivileged user can add/modify the Invoices/Sales Orders/Items/Customers/ Quotes fields parameter to inject arbitrary JavaScript.	N/A	A-NCH-EXPR- 041119/360
			CVE ID : CVE-2019- 16330		
Netapp	•				

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	1-2	7	†) †	3-0	0-7	7	5	J-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
snapmanage	r		L		
N/A	16-10-2019	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-SNAP- 041119/361
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			by an 3.0 Ba (Avai: CVSS (CVSS N/UI: CVE I	(e.g., cod adminis ase Score lability in Vector: S:3.0/AV R/S:U/C D: CVE-	trator). 2 3.1 2 3.1 2 3.1 3 3.1 3 3.1 4 3.1 5 3.1 5 3.1 6 3	CVSS . I/PR: A:L). 945 va				
N/A	16-10-2019	4.3	produ (com) Suppo are af 7u23 13; Ja 8u22 vulne unaut with a Kerbe Java S Embe vulne Java S additi Succe vulne unaut critica acces SE En data. vulne Java S additi succes succes se En data.	va SE Em act of Ora ponent: I orted ver fected an 1, 8u221 ava SE Em 1. Difficu rability a thenticat retwork eros to co SE, Java S edded. W rability i orability o thorized al data or s to all Ja abedded Note: The rability a leploymo ally in cli oxed Jav cations o applets (i oad and	Kerbero rsions the re Java S , 11.0.4 hbedded alt to expended attack access we comprom E hile the dded, at htly impleducts. acks of the can resu access the access th	a SE s). nat sE: and d: cloit eker via nise a SE, tacks act chis lt in o ete ava ble co nning Start oxed	https://sty.netapi /advisor p-20191 0001/	p.com ry/nta	A-NET-: 041119	
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	D	escription	& CVE II	D	Pato	h	NCIIP	CID
			that contents of the composition	sted codomes fromet) and such andbox for and	om the rely on the rely on the for seculility can y using degarders. Through the A Score 6 ty impacts of the A Score 6 ty impacts of the	the rity. also APIs ugh a PIs8 cts). I/PR: A:N).				
N/A	16-10-2019	5.8	Vulne SE prosection SE (consumption SE (consum	erability is oduct of omponer orted verificated and 13. it vulners is unauthoris via multiple of the color of	in the Ja Oracle J Oracle J Int: Hotsp rsions the re Java S Difficult ability enticate metwork tiple omprom ssful att ability ca thorized a subse ible dat ized abilitial deni al DOS) This applies tents, ents run va Web S	va ava ava bot). hat EE: t to ed cacks an d et of a lity hal of of co ming Start	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-: 041119	
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	D	escription	a & CVE I	D	Pato	h	NCIIP	CID
			that lead that control interrest apply typical load a code by an 3.0 Ba (Conf Availa Vector)	pplets (in pad and and sted code omes from the code of	run e (e.g., com the rely on for secuility doe deploymers, the only trusted trator). e 4.8 ty and apacts).	code the rity. es not nents, nat sted led CVSS CVSS				
				D : CVE-						
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En attack vulne unaut cause service Java S	rability in a SE Empore of Oract of Oract of Oract of Oract of Oract of Empore of the oract of this rability of the oract of the oracl of the oracle of the ora	nbedded acle Java Network rsions the re Java S , 11.0.4 nbedded lt to exp allows access vacces to ava SE, J . Succes can resu ability to l denial al DOS)	I a SE king). nat SE: and d: oloit ker via [ava sful of of	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-: 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			Java de typica sandhapplica Java a that le untru that continue in the Compared Supplication (Available CVSS (CVSS N/UI:		ents, ents rur va Web S r sandb in Java S run le (e.g., c om the rely on t for secu ility can by using d le d le d le to the A Score 3 mpacts) EN/AC:H	nning Start oxed oxed iE 8), code the rity. also APIs ugh a PIs. 7 I/PR: A:L).				
N/A	16-10-2019	4.3	N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2978 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in				https://sty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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			Pato	:h	NCIIP	NCIIPC ID	
			cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2981							
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to			https://securi ty.netapp.com /advisory/nta p-20191017- 0001/		A-NET-SNAP- 041119/366		
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			Pato	h	NCIIP	C ID	
			SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2983							
N/A	16-10-2019	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network			https://securi ty.netapp.com /advisory/nta p-20191017- 0001/		A-NET-SNAP- 041119/367		
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	D	escription	ո & CVE I	D	Pato	:h	NCIIP	CID
			access proto Java S of this result ability denia DOS) vulne Java a that le untru that c interr Java s This v be expin the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	s via muicols to constitution of Java Strability and and sted code omes from the ploited by specific onent, energical and sted code omes from the ploited by specific onent, energical and sted code ones from the ploited by specific onent, energical and sted code ones from the ploited by specific onent, energical and sandbox will be specifically in the ploited by specific	ltiple ompron ssful att ability can be a part ice (part ice (part ice) (part	nise cacks an d ial tial tial trial Start oxed SE 8), code the rity. also APIs ugh a PIs. 3.7 . 4/PR: (A:L).				
N/A	16-10-2019	4.3	SE, Japrodu (composuppo are af 7u23: 13; Ja 8u22:	erability va SE En ponent: 2 ported ver fected an 1, 8u221 va SE En 1. Difficu	nbedded acle Java 2D). rsions the re Java S ., 11.0.4 nbedded	l a SE nat SE: and l:	https://sty.netapy/advisorp-201910001/	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIF	CID
			unaut	henticat	ed attac	ker				
			with 1	network	access v	<i>r</i> ia				
			multi	ple proto	ocols to					
			comp	romise J	ava SE, J	lava				
			SE En	nbedded	. Succes	sful				
			attack	ks of this						
			vulne	rability (can resu	lt in				
			unaut	horized	ability t	0				
			cause	a partia	l denial	of				
			servio	e (partia	al DOS)	of				
			Java S	E, Java S	E					
			Embe	dded. No	ote: This	5				
			vulne	rability a	applies t	0				
			Java d	leploym	ents,					
			typica	ally in cli	ents rur	nning				
			sandb	oxed Jav	7a Web S	Start				
			applio	cations o	r sandb	oxed				
			Java a	pplets (i	n Java S	E 8),				
			that l	oad and	run					
			untru	sted cod	le (e.g., c	ode				
			that c	omes fro	m the					
			interr	net) and	rely on	the				
			Java s	andbox	for secu	rity.				
			This v	<i>r</i> ulnerab	ility doe	es not				
			apply	to Java	deploym	ients,				
			J 1	ally in se	•					
				ınd run o						
			code	(e.g., cod	e install	led				
			by an	adminis	trator).	CVSS				
			3.0 Ba	ase Score	e 3.7					
			(Avai	lability ii	mpacts)					
			CVSS	Vector:						
			(CVSS	5:3.0/AV	:N/AC:H	I/PR:				
			N/UI:	N/S:U/C	::N/I:N/	A:L).				
			CVE I	D : CVE-	2019-2	988				
			Vulne	rability	in the O	racle	https://	securi		
			Graal	VM Ente	rprise		ty.netap			
N/A	16-10-2019	4.3	Edition product of Oracle				/advisoi	_	A-NET-	
/	10 10 2017	1.0	GraalVM (component:				p-20191		041119	/369
			Java).	The sup	ported		0001/			
			versio	on that is	affecte	d is				
CV Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				1/6						

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			19.2.0 vulne unaut with r multip comp Graal' Edition signif additi Succe vulne unaut deleti access Oracle Edition CVSS (Integ Vecto (CVSS N/UI:	D. Difficult rability and thenticate then the protocomise (Normal Protocom). While the protocom attack is and protocom access to critical protocom access 3.0 Base grity imports (1.3.0/AV N/S:C/C	It to expallows access we cools to Oracle rprise in Oracle reation oddification call data in Entersible data in Score 6 in acts). CV	loit ker via cle his lt in or all prise a8 VSS				
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful				https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
			וום בט	aucu	. Jaccos	5141				

Weakness	Publish Date	CVSS	D	escription	ı & CVE I	D	Pato	:h	NCIIP	CID
			vulne unaut cause service Java S Embe vulne Java d typica sandhat le untru that c interred Java s This vapply typica load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	as of this rability of thorized a partial se (partial	can resurability to ability to ability to all DOS) of E conternations of the content of the cont	of o				
N/A	16-10-2019	4	SE, Japrodu (composupposupposupposupposupposupposuppos	erability to a SE Emore of Oraconent: orted versed is Javant to expend to ex	nbedded acle Java The rsion tha a SE: 8u dded: 8u ploit allows	l a SE at is 221; 1221.	https://sty.netapgi /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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	D	escriptio	n & CVE I	D	Patc	h	NCIIP	C ID
			with	network	access v	<i>r</i> ia				
			multi	ple prote	ocols to					
			comp	romise J	ava SE, J	lava				
			SE En	nbedded	. Succes	sful				
			attacl	ks requir	e huma	n				
			intera	action fr	om a pei	rson				
			other	than the	e attacke	er.				
			Succe	ssful att	acks of t	his				
			vulne	rability	can resu	lt in				
			unau	thorized	update,					
			inser	t or dele	te access	s to				
			some	of Java S	SE, Java S	SE				
			Embe	edded ac	cessible	data				
			as we	ll as una	uthoriz	ed				
			read a	access to	a subse	et of				
			Java S	SE, Java S	SE Embe	dded				
			acces	sible dat	a. Note:	This				
			vulne	rability	applies t	to				
			Java d	leploym	ents,					
			typica	ally in cli	ents rui	nning				
			sandl	oxed Jav	va Web S	Start				
			appli	cations c	r sandb	oxed				
			Java a	ipplets (in Java S	E 8),				
			that l	oad and	run					
			untru	sted cod	le (e.g., c	code				
			that c	omes fro	om the					
			interi	net) and	rely on	the				
			Java s	andbox	for secu	rity.				
			This	zulnerab	ility doe	es not				
			apply	to Java	deployn	nents,				
			typica	ally in se	rvers, th	nat				
			load a	and run (only trus	sted				
			code	(e.g., cod	le install	led				
				adminis						
			_	ase Score	•					
			(Conf	identiali	ty and					
			(Confidentiality and Integrity impacts). CVSS							
			Vector:							
			(CVSS:3.0/AV:N/AC:H/PR:							
			N/UI:R/S:U/C:L/I:L/A:N).							
			CVE ID : CVE-2019-2996							
CV Scoring Scale	<u> </u>									
(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
N/A	16-10-2019	4	Vulnerability in the Java SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-SNAP- 041119/372

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			typical load a code by an 3.0 Ba (Confintegrate) Vector (CVSS N/UI:	to Java of ally in seand run of the control of the	rvers, the only trusted install trator). e 4.7 ty and acts). CV::N/AC:H	nat sted led CVSS 'SS I/PR: A:N).				
N/A	16-10-2019	4.3	SE, Japrodu (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En attack vulne unaut deleti acces Java Sacces vulne Java of typica sandk applica Java a fava a fa	erability in a SE Emponent: In ponent: In po	acle Java Scients of the J	I SE s). nat SE: and d: cloit cker via lava sful dt in n, or all dded This to nning Start oxed	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
CV Scoring Scal	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			that contents of the explication of the composition	sted codomes fromet) and andbox rulnerab ploited be specified be revice where the data 3.0 Base grity imports: 5:3.0/AV N/S:U/C D: CVE-	om the rely on the rely on the for seculility can be using the description of the Alexandry Score 5 to acts). Currently Score 5 to acts (Sintal Cintal Cinta	the rity. also APIs ugh a PIs9 VSS I/PR: A:N).				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with multicomp SE En attack vulne unaut cause service Java SEmber vulne Java de	erability va SE En oct of Ora ponent: 2 orted ver fected an 1, 8u221 va SE En 1. Difficu- rability a chenticat hetwork ple proto romise J hobedded as of this rability o chorized a partia ce (partia ce (partia de (partia) de (partia)	in the Janbedded acle Java 2D). rsions the Java Son Java Son Java Son Java Son Java Sed attaction access where Java Sed attaction are sun ability to the Java Sed attaction and DOS) of the Java Sed attaction and DOS) of the Java Sed attaction and DOS) of the Java Sed applies to the Java Sed attaction and Java Sed attactio	va l I SE nat E: and d: cloit eker via sful lt in o of of	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-: 041119	
CV Scoring Sca	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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			applied Java at that let untrue that continued in the Composite of the Com	cations of applets (in pad and and and and and and and and and a	or sandb in Java S run le (e.g., com the rely on for secu ility can by using d .g., throw which to the A Score 3 mpacts)	oxed SE 8), code the rity. also APIs ugh a PIs. 3.7				
N/A	16-10-2019	4.3	Vulnes SE, Ja produ (comp Concu versic are Ja 11.0.4 Embe Diffic vulne unaut with i multi comp SE En attack vulne unaut cause	erability va SE Emuct of Oraponent: arrency) ons that a va SE: 70 and 13 edded: 80 and 13 ethenticate ple protographic of this erability of thorized a partiace (partial	in the Janbedded acle Java . Support are affect 1231, 8th 1221. In ploit allows access to access to ava SE, Java SE, Ja	rted cted u221, cker via Java sful ult in co	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			Emberoulne explored data to specific without Java Wapplic Java athrout CVSS (Avail CVSS (CVSS N/UI:	SE, Java Sedded. No rability of ited by second complets of the second complets, second complete, second comp	ote: This can only upplyin the ponent Untrust t r Untrus o service Score 3 mpacts) :N/AC:H	ted sted .7 . (/PR: A:L).				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with multip comp SE En attack vulne unaut cause service Java S Embe vulne	erability in a SE Emuct of Orac ponent: Jorted verificated and 1, 8u221 va SE En 1. Difficulting a chorized a partial ce (partial se (part	in the Janbedded acle Java (AXP). The Java Strain s	va I SE nat EE: and It: oloit eker via fava sful It in of of	https://sty.netapg /advisor p-20191 0001/	p.com ry/nta	A-NET-9	
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	Publi	ish Date	cvss	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	CID
				sandbapplic Java a that le untru that cointern Java so This was in the Compweb so supplicity (Avail CVSS (CVSS N/UI:	cations of applets (poad and asted coordinated coordinated and andbox vulnerable) and andbox vulnerable specifies data 3.0 Base lability i Vector: S:3.0/AV N/S:U/O	de (e.g., com the rely on for secupility can be secupility.	Start oxed EE 8), code the rity. also APIs ugh a PIs7 . I/PR: A:L).				
N/A		0-2019	5.8	SE, Ja produ (comp Suppo are af 8u22 SE En Diffic vulne unaut with a multi comp SE En attack vulne unaut	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to				securi p.com ry/nta .017-	A-NET-: 041119	
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
			Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L). CVE ID: CVE-2019-2975		
snapcenter					
Information Exposure	16-10-2019	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-NET-SNAP- 041119/378
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
			attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N).		
Information Exposure	16-10-2019	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2924	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-NET-SNAP- 041119/379
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
oncommand	_workflow_aut	omatio	on		
Information Exposure	16-10-2019	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2922	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-NET-ONCO- 041119/380
N/A	16-10-2019	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-ONCO- 041119/381

1-2

0-1

CV Scoring Scale

4-5

3-4

5-6

6-7

7-8

8-9

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			SE En	nbedded	. Succes	sful				
			attacl	ks requir	e huma	n				
				action fro	_					
				than the						
				ssful att						
				rability (
				thorized	•					
			cause	a partia	l denial	of				
				ce (partia	-	of				
			-	SE, Java S						
				dded. No						
				rability a		0				
				leploym						
				ally in cli		_				
				oxed Jav						
				cations o						
				ipplets (i		E 8),				
				oad and						
				sted cod		ode				
				omes fro						
				net) and	-					
				andbox		-				
				ulnerab/	-					
				to Java						
				ally in se						
				and run o						
				(e.g., cod						
			_	adminis	_	CVSS				
				ase Score						
			-	lability i	mpacts)					
				Vector:						
			-	5:3.0/AV	-	-				
			N/UI:	R/S:U/C	::N/I:N/	A:L).				
			CVE I	D : CVE-	2019-2	945				
			Vulne	rability	in the Ja	va				
			SE, Ja	va SE En	bedded	l	https://	securi		
			produ	ict of Ora	acle Java	a SE	ty.netap	p.com	A-NET-	ONCO-
N/A	16-10-2019	4.3	(com	ponent: l	Kerbero	s).	/advisoi		041119	
			Supp	orted ve	rsions th	nat	p-20191	.017-	OTILIA	1502
			are af	fected a	re Java S	E:	0001/			
			7u23	1, 8u221	, 11.0.4	and				
CV Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				150						

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			13; Ja	ıva SE Er	nbedde	d:				
			8u22	1. Difficu	ılt to exp	oloit				
			vulne	rability	allows					
			unau	thentica	ted attac	cker				
			with	network	access	via				
			Kerb	eros to c	ompron	nise				
			Java S	SE, Java S	SE					
			Embe	edded. W	hile the	!				
			vulne	rability	is in Java	a SE,				
				SE Embe						
			· ·	significa						
			-	ional pro						
				essful att		this				
				rability						
				thorized						
				al data o						
				s to all Ja	_					
				nbedded						
				Note: Th		DIC				
				rability		to				
				deploym						
				ally in cl		nnina				
				ooxed Ja		_				
				cations (
				applets (
			-	• •	•	oe oj,				
				oad and						
				isted cod		coae				
				comes fr		.,				
				net) and	_					
				sandbox		-				
				vulnerab	•					
				ploited l		APIs				
				e specifie						
			_	onent, e	•	ugh a				
			web s	service v	vhich					
			supp	lies data	to the A	PIs.				
			CVSS 3.0 Base Score 6.8							
			(Conf	fidential	ty impa					
			CVSS	Vector:						
			(CVS	S:3.0/AV	:N/AC:H	I/PR:				
			N/UI	:N/S:C/0	:H/I:N/	A:N).				
				1						
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2949		
N/A	16-10-2019	5.8	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.8 (Confidentiality and Availability impacts). CVSS	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-ONCO- 041119/383
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			N/UI:	or: 5:3.0/AV N/S:U/C D : CVE -	:L/I:N/	Á:L).				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En attack vulne unaut cause service Java SEmber vulne Java	erability va SE En oct of Or ponent: orted ve fected a 1, 8u221 va SE Er 1. Difficu rability chenticat network ple prote romise J nbedded as of this orability chorized a partia ce (partia se, Java Se edded. Ne rability chorized a partia ce (partia ce (p	nbedded acle Java Network rsions the rsions the rejava S., 11.0.4 abedded attacked ability to ability to applies the results runder sandbar sandb	d SE king). hat SE: and d: bloit cker via Java sful dit in to of sto mning Start oxed SE 8), code the rity. halso APIs	https://sty.netapj /advisor p-20191 0001/	p.com ry/nta	A-NET-0 041119	
CV Scoring Sca (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				Pato	:h	NCIIP	C ID
			suppl CVSS (Avai CVSS (CVSS N/UI CVE I	service wata 3.0 Base lability i Vector: 5:3.0/AV: N/S:U/C	to the A Score 3 mpacts) :N/AC:F ::N/I:N/	i.7 I/PR: A:L). 978				
N/A	16-10-2019	4.3	production (com Support of Suppor	va SE Enuct of Or ponent: orted verificated a 1, 8u221 ava SE Enucharicated and a partial ace (partial SE, Java Sedded. Nerability ally in classifications of applets (poad and asted comes fronet) and sandbox	acle Java JAXP). rsions the re Java St., 11.0.4 mbedded alt to expend allows ted attack access who cols to fava SE, just a bility the lents of the sandbury and we be soon the rely on the rely of the rely on the rely of the rely on the rely on the rely of the	a SE nat SE: and d: cloit cker via lava sful dt in co of sto nning Start oxed SE 8), code the	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-041119	
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
			be exin the Compweb's supplicities (Avai CVSS (CVSS N/UI:	vulnerable ploited be specified to service whites data 3.0 Base lability i Vector: S:3.0/AV	oy using ed e.g., throwhich to the A e Score 3 mpacts) E:N/AC:HE:N/I:N/	APIs ugh a PIs. 3.7 . I/PR: (A:L). 981				
N/A	16-10-2019	4.3	SE, Ja produ (com Serial versic are Ja 11.0.4 Embe Diffic vulne unaut with multi comp SE En attack vulne unaut cause servic Java S Embe vulne Java G typica sandk applic	erability va SE En act of Or ponent: lization) ons that va SE: 7 4 and 13 edded: 8 ult to ex erability thentical network ple prote oromise J nbedded ex of this erability thorized ex a partia ce (parti SE, Java S edded. N erability deploym ally in cl poxed Jav cations of applets (nbedded acle Java acle Java are affect u231, 80 ; Java SE u221. ploit allows ted attact access to cools to ava SE, ability to allows ability to allows ability to allows applies applies applies applies applies are and bor sandbor s	ted cted 1221, Eker via Sful lit in co of cto chaning Start oxed	https://ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET-041119	
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	D	escription	ı & CVE I	D	Pato	h	NCIIP	CID
			untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	oad and sted cod omes fromet) and andbox and	e (e.g., com the rely on for secular ility can be using defined as the secular in the A score 3 mpacts) :N/AC:H	the rity. also APIs ugh a PIs7 . I/PR: A:L).				
N/A	16-10-2019	4.3	Vulne SE prosection SE (consumption SE (consum	erability in oduct of omponer orted verificated and 13 it vulner is unauth it ser with its via multiple of Java Serability and leployment of J	in the Jacobia Oracle Jacobia Science Java Scienticate on the Itiple ompronessful attached a partice (partice (partice (partice) (partice) on the Itiple on the Itiple of	va ava at EE: t to ed cacks an d ial cial This co nning Start oxed	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
			that contents of the composition	N/S:U/C	om the rely on the rely on the for seculility can be using the desired of the Alexandra Score 3 mpacts) :N/AC:H :N/I:N/	the rity. also APIs ugh a PIs7 . I/PR: A:L).				
N/A	16-10-2019	4.3	(CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2987 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This				https://sty.netapy/advisorp-201910001/	p.com y/nta	A-NET-0 041119	
				leploymo ally in cli		nning				

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			application applies a that lead to the control of t	cations of applets (in pad and sted code omes from and so and so and so and so and run of administics as Score lability in Vector: S:3.0/AV N/S:U/O D: CVE-	or sandb in Java S run le (e.g., com the rely on the rely on the ility doe deploymervers, the only truste installetrator). e 3.7 impacts)	oxed E 8), code the rity. es not nents, at sted ed CVSS				
N/A	16-10-2019	4.3	Vulne Graal Edition Graal Java). version 19.2.0 vulne unaut with in multing comp Graal Edition vulne Graal Edition significated	erability VM Ente on produ VM (com The sup on that is chenticat network ple proto romise (VM Ente on, While icantly in ional pro- essful attar rability (in the Or rprise ct of Ora ponent ported s affected by the allows access we pocols to Oracle rprise the is in Ora rprise as may mpact oducts. acks of t	racle acle d is doit ker via	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
		deleti acces Oracl Editio CVSS (Integ Vecto (CVSS N/UI	thorized ion or m s to criti e GraalV on access 3.0 Base grity imp or: S:3.0/AV :N/S:C/C	odificati cal data 'M Enter sible dat e Score 6 pacts). C' :N/AC:H	on or all or all or prise a. 5.8 VSS VSS I/PR: A:N).				
N/A 16-10-2019	4.3	SE, Ja produ (com Supplare at 7u23 13; Ja 8u22 vulne unau with multi complete service Java Service Java Service Java Service sandi applicate at tat I	erability va SE En uct of Or ponent: orted ve ffected a 1, 8u221 thentical network ple prote oromise J nbedded as of this erability thorized e a partia ce (parti SE, Java S edded. N erability deploym ally in cli coxed Jav cations o applets (oad and asted coc steed coc asted coc asted coc asted coc	nbedded acle Java 2D). rsions the re Java S 1, 11.0.4 nbedded alt to exp allows ted attace access versions to ava SE, j l. Succes can resurability tel al DOS) SE ote: This applies te ents, ients run va Web S or sandb in Java S run	a SE nat SE: and d: cloit cker via Java sful dt in co of of sto nning Start oxed SE 8),	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-0 041119	
CV Scoring Scale (CVSS)	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			interr Java s This v apply typica load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	omes fromet) and andbox and and and run of the contract of the	rely on to for secu- ility doe deploym rvers, the only trus e install trator). e 3.7 mpacts) :N/AC:H	rity. es not nents, nat sted ed CVSS . I/PR: A:L).				
N/A	16-10-2019	4	SE, Jar produ (composupposupposupposupposupposupposuppos	rability va SE Em act of Ora conent: yment). orted ver ed is Jav E Embed ult to exp rability a chenticat network ple proto romise J nbedded as requir action fro than the asful attra chorized or delet of Java S dded acc ll as una	The rsion that a SE: 8u dded:	at is 221; 221. Eker via sful ner. Ehis lt in SE data	https://sty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-041119	
			read a	access to		t of				

Weakness	Publish Date	CVSS	D	escription	1 & CVE II	D	Pate	ch	NCIIP	CID	
			Java S access vulne Java d typica sandh applic Java a that le untru that c interr Java s This v apply typica load a code (by an 3.0 Ba (Conf Integr Vecto (CVSS N/UI:	EE, Java Sible dat rability a leploymonally in clipoxed Java cations of a leploymonally in second and box and box a leploymonally in second administrate Score identiality imparts: E:3.0/AV R/S:U/C	EE Embera. Note: applies to ents, ents run le (e.g., combing Java Strun le (e.g., combing the rely on	dded This to nning Start oxed E 8), tode the rity. ts not nents, at ed CVSS					
N/A	16-10-2019	4	Vulnerability in the Java SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the				https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119		
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	D	escription	n & CVE I	D	Pato	h	NCIIP	PC ID
Weakness	Publish Date	CVSS	attack vulne attack impact productions attack vulne unaut insert some data a unaut to a staces; vulne Java data a that le untru that content java so This vapply typical load a code by an 3.0 Ba (Confintegral Vector (CVSS)	ser and verability in a ser addition of Java Ser ability of a ser ability of a ser and a ser and box a ser and and box a ser and run of a ser a	while the is in Java ignificar on al cessful can resu update, te access read access read access and when the in Java Serun le (e.g., com the rely on for secu ility doe deploymers, the only truste install strator). e 4.7 ty and acts). CV	e a SE, atly alt in s to sible cess This to ming Start oxed E 8), code the rity. es not nents, at sted led CVSS	Patc	:h	NCIIP	PCID
			N/UI:R/S:C/C:L/I:L/A:N). CVE ID : CVE-2019-2999							
N/A	16-10-2019	4.3	SE, Java SE Embedded		https://s ty.netapy /advisor	p.com	A-NET- 041119			
CV Scoring Sca (CVSS)	o-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(component: Libraries). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:	Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
are affected are Java SE: 7u231, 8u221, 11.04 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				(com	ponent:	Librarie	s).	p-20191	017-		
7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				Supp	orted ve	rsions th	nat	0001/			
13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that Joad and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				are af	fected a	re Java S	SE:				
8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				7u23	1, 8u221	1, 11.0.4	and				
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				13; Ja	va SE Er	nbedded	d:				
unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				8u22	 Difficι 	ılt to exp	oloit				
with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				vulne	rability	allows					
multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				unau	thentica	ted attac	cker				
compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				with	network	access	<i>r</i> ia				
SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				multi	ple prot	ocols to					
attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				comp	romise J	ava SE, j	Java				
vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				SE En	nbedded	l. Succes	sful				
unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				attacl	ks of this	5					
deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				vulne	rability	can resu	ılt in				
access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				unau	thorized	creation	n,				
Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				deleti	ion or m	odificati	on				
accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				acces	s to criti	cal data	or all				
accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				Java S	SE, Java S	SE Embe	dded				
Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				1	-						
Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				vulne	rability	applies 1	to				
typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:					_						
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:							nning				
applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:					-		_				
Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:											
that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:											
untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS				· .	• • •	•	,				
that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:							code				
Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:											
Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				interi	net) and	rely on	the				
This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:					-	-					
be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:							-				
in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:						-					
Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:					•		711 15				
web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:					•		ugh a				
supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:				-		•	ugii u				
CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector:							DIc				
(Integrity impacts). CVSS Vector:											
Vector:											
				, ,		iacisj. G	۷ کی				
[(CV55:5.U/AV:N/AC:П/PK:						.NI /AC.I	ı/DD.				
				-	•	•	-				
N/UI:N/S:U/C:N/I:H/A:N).				IN/UI:	.1N/2:U/(.:IN/I:H/	A:NJ.				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 5	CV Scoring Sca	ile 0-1	1-2	2-2	3_//	/l_5	5-6	6-7	7_9	Q_Q	9-10

(CVSS)

Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.				CVE ID : CVE-2019-2958		
	N/A	16-10-2019	4.3	SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.	ty.netapp.com /advisory/nta p-20191017-	A-NET-ONCO- 041119/394

Weakness	Publish Date	CVSS	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
			(Avail CVSS (CVSS N/UI: CVE I Vulne SE, Jar produ (comp Concu versic are Ja 11.0.4 Embe Diffict vulne unaut with i multip comp SE En attack	escription lability in Vector: 5:3.0/AV: 6:3.0/AV: 6:3.0	mpacts). :N/AC:H :N/I:N/I 2019-2 in the Ja nbedded acle Java . Support are affect u231, 8u ; Java SE u221. ploit allows access v ocols to ava SE, J . Success	i/PR: A:L). 962 va l a SE rted cted a 221, cker via ava sful	https://ty.netap	securi p.com	A-NET-0	
N/A	16-10-2019	4.3	cause service Java S Embe vulne explo data t specification Java V applice Java a throu CVSS (Avail CVSS	thorized a partial ce (partial	l denial al DOS) of E ote: This can only upplyin the ponent Untrust t or Untrus such as o service Score 3 mpacts)	of of of sted sted c. 7	/advisor p-20191 0001/		041119	/395
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			N/UI:	N/S:U/C	:N/I:N/	A:L).				
			CVE I	D : CVE-	2019-2	964				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppor are aff 7u23 13; Ja 8u22 vulne unaut with a multi comp SE En attack vulne unaut cause service Java SEmber vulne SEMBER V	rability va SE En oct of Oraconent: Jorted verificated and see (partial E, Java See (partial	nbedded acle Java (AXP). It is a Java State attaction and access where the color is a policy and be seen ability to a many a Web State and be seen and be seen and be seen and be seen and be a large of the color in Java Strum be seen and be seen a	a SE at E: and d: bloit ker via ava sful lt in o of of start oxed E 8), code the rity. also APIs ugh a	https://sty.netapy/advisorp-201910001/	p.com y/nta	A-NET-0 041119	
	1		_ ^ ^							

Weakness	Publish Date	cvss	D	escription	ı & CVE II	D	Pato	:h	NCIIP	C ID
			(Avail CVSS (CVSS N/UI: CVE I	3.0 Base lability in Vector: 6:3.0/AV: N/S:U/C D: CVE-erability in the second control of	mpacts). :N/AC:H ::N/I:N/. 2019-2 in the Ja	I/PR: A:L). 973 .va				
N/A	16-10-2019	5.8	produ (com) Suppo are af 8u22: SE En Diffici vulne unaut with in multi comp SE En attack vulne unaut insert some Embe and u to cau service Java S Embe vulne Java d typica sandk applica Java a that le untru	va SE Emarct of Oraponent: Sorted vera fected and all to expended and all to expended according to a particle (partial sea a particle (particle (p	acle Java Scripting rsions the re Java S and 13; : 8u221. ploit allows ed attace access v ocols to ava SE, J . Success can resu update, te access EE, Java S cessible ized abil tial deni al DOS) of EE ote: This applies t ents, ents run va Web S or sandbe in Java S run le (e.g., c	s SE g). nat SE: Java Java sful alt in SE data lity ial of of sto Start oxed SE 8),	https://s ty.netapj /advisor p-20191 0001/	p.com y/nta	A-NET-0 041119	
	ale 0.4									

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L). CVE ID: CVE-2019-2975		
element_soft	 ware_manage	ment_r	node		
Improper Input Validation	17-10-2019	9	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#\$((0xffffffff))" command. CVE ID: CVE-2019-14287	https://securi ty.netapp.com /advisory/nta p-20191017- 0003/, https://suppo rt.f5.com/csp /article/K537 46212?utm_s ource=f5supp ort&utm _medium=RSS , https://www. sudo.ws/alert s/minus_1_ui d.html	A-NET-ELEM- 041119/398
e-series_sant	ricity_os_cont	roller			
N/A	16-10-2019	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE:	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/399
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

7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that Ioad and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:R/S:U/C:N/I:N/A:L).	Weakness	Publish Date	cvss	Descripti	on & CVE I	D	Pato	h	NCIIP	CID
8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				7u231, 8u22	21, 11.0.4	and				
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				13; Java SE E	Embedded	d:				
unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				8u221. Diffic	cult to exp	oloit				
with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS: 3.0/AV:N/AC:H/PR:				vulnerability	allows					
multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS'3.0/AV:N/AC:H/PR:				-		cker				
compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				with networ	k access v	<i>r</i> ia				
compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				multiple pro	tocols to					
SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				• •		lava				
interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:				-	-					
interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:				attacks requ	ire huma	n				
other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:				_						
vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					-					
vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				Successful a	ttacks of t	his				
unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-						
service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					-					
Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-						
Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS: 3.0/AV:N/AC:H/PR:				7-	-	01				
vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-		10				
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				= -						
applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						_				
Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					•	E 8J,				
that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						,				
internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						code				
Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-	_					
apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				*		-				
typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					_					
load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				typically in s	ervers, th	nat				
by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				load and run	only tru	sted				
3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				code (e.g., co	de install	led				
(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				by an admin	istrator).	CVSS				
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				3.0 Base Sco	re 3.1					
(CVSS:3.0/AV:N/AC:H/PR:				(Availability	impacts)					
				CVSS Vector	:					
N/UI:R/S:U/C:N/I:N/A:L).				(CVSS:3.0/A	V:N/AC:H	I/PR:				
				N/UI:R/S:U/	'C:N/I:N/	A:L).				
CV Scoring Scale										

(CVSS)

Weakness	Publish Date	cvss	Description	on & CVE II	D	Pato	h	NCIIP	C ID
			CVE ID : CVE	E-2019-2	945				
N/A	16-10-2019	4.3	Vulnerability SE, Java SE E product of O (components Supported ve are affected a 7u231, 8u22 13; Java SE E 8u221. Diffic vulnerability unauthentica with network Kerberos to Java SE, Java Embedded. V vulnerability Java SE Embedded additional pr Successful at vulnerability unauthorize critical data access to all SE Embedde data. Note: T vulnerability Java deployn typically in c sandboxed Ja applications Java applets that load and untrusted co that comes fi internet) and Java sandbox This vulnera be exploited in the specifi	mbedded racle Java Kerbero ersions the are Java S 1, 11.0.4 mbedded rult to experience of the area of	I SE s). That SE: That SE, That S	https://ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	h Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				web s suppl CVSS (Conf CVSS (CVSS N/UI CVE I	service values data 3.0 Base idential Vector: S:3.0/AV:N/S:C/C	to the A e Score 6 ity impa ':N/AC:H C:H/I:N/	PIs. 5.8 cts). I/PR: A:N).				
N/A	16-10-	2019	5.8	SE pr SE (co Supp are at 11.0.4 explor allow attack acces proto Java S of thi result read Java S and u to cau servic Java S vulne Java G typica sandl appli Java a that l untru that o interr Java S	oduct of ompone orted verificated a 4 and 13 at vulner with s via much ocols to compare to in unautaccess to Eaccess inauthor use a particle. Note: erability deployment of the compare to	nenticated network litiple compronessful attability can be a subsection of a s	ava pot). hat EE: It to ed k hise cacks an d et of a lity ial of of to nning Start oxed EE 8), code the rity.	https://s ty.netapj /advisor p-20191 0001/	o.com y/nta	A-NET-I 041119	
CV Scoring Sca (CVSS)	ie (0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			typical load a code by an 3.0 Ba (Conf Availa Vecto (CVSS N/UI:	to Java of ally in second run of the control of the	rvers, the only trusted install trator). 4.8 ty and apacts).	at sted ed CVSS CVSS I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Japrodu (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En attack vulne unaut cause service Java S Embe vulne Java of typica sandk applice Java a a general sandk applice Java a general sandk a general s	erability in a SE Emuct of Oraponent: It or ted verificated and a second and and a second and and a second and and a second a second and a second	nbedded acle Java Network rsions the sions the sions the sions the sions access where the sions access where the sions access where sions to ava SE, Jan Cols to ava S	s SE king). at SE: and d: bloit ker via at sful It in o of of of of and start oxed	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
CV Scoring Scal	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
			that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	sted code omes from the comes from the contract of the contrac	om the rely on to for securility can by using degree de degree de	the rity. also APIs ugh a PIs7 . (/PR: A:L).				
	1			erability						
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with I multip comp SE En attack vulne unaut cause service Java S Embe vulne Java d	va SE Emuct of Oraponent: Jorted verificated and 1, 8u221 va SE End 1. Difficult achenticated a partial ce (partial ce (partia	acle Java (AXP). rsions the re Java S , 11.0.4 abedded alt to exp allows red attac access v ocols to ava SE, J . Success can resu ability t I denial al DOS) of E ote: This	a SE at EE: and d: cloit eker via fava sful lt in o of of	https://sty.netapy/advisorp-201910001/	p.com y/nta	A-NET-1 041119	
			J 1	illy ill cit	circo i ai					

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			applied Java at that let untrue that continued in the Comparent of the Com	cations of applets (in pad and and asted code and	or sandb in Java S run le (e.g., com the rely on for secu ility can by using d .g., through thich to the A Score 3 mpacts)	oxed SE 8), code the rity. also APIs ugh a PIs. 3.7				
N/A	16-10-2019	4.3	Vulne SE, Ja produ (comp Serial versical are Ja 11.0.4 Ember Diffical vulne unaut with multi comp SE En attack vulne unaut cause	erability va SE Emuct of Oraponent: lization). ons that a va SE: 70 and 13 edded: 80 and 13 edded: 80 and 14 and 15 edded as of this rability of thorized a partial ce (partial ce (partia	in the Janbedded acle Java Support are affect at 1221. ploit allows access to ava SE, Java SE	tva It a SE Tted cted u221, E cker via Java sful ult in co of	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	PC ID
			Embervulne Java de typical sandha applical Java a that le untrue that continue in the Complex Supplication (Available CVSS (CVSS N/UI:	EE, Java Sedded. No rability a leploymore ally in clip oxed Java Sations of applets (in oad and asted code and andbox aulnerabe ploited be specified onent, expecified sations of a sations of a specified sat	ote: This applies to ents, dents run le (e.g., com the rely on the rely on the degree of the A score 3 mpacts) :N/AC:H	nning Start oxed E 8), code the rity. also APIs ugh a PIs7 .				
N/A	16-10-2019	4.3	SE prosection SE prosection SE (construction SE (construc	erability oduct of omponer orted ver fected and 13 it vulner is unauth s via mu cols to co E. Succe s vulner it in unau y to caus	Oracle Jat: 2D). It: 2D). It: 2D). It: 2D). It: 2D	ava nat EE: t to ed cacks an d ial	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIF	CID
			vulne Java d typica sandh applic Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	of Java S rability a leployme ally in cli boxed Jav cations o applets (i boad and sted cod omes fro andbox i vulnerab ploited b especifie conent, e ervice w ies data 3.0 Base lability in Vector: S:3.0/AV N/S:U/O D: CVE-	applies tents, lents rur va Web S or sandb in Java S run le (e.g., com the rely on te for secu ility can by using d le g., throughtouth to the A Score 3 mpacts) :N/AC:H C:N/I:N/	nning Start oxed E 8), code the rity. also APIs ugh a PIs7 . (/PR: A:L).				
N/A	16-10-2019	4.3	SE, Japrodu (composupposupposupposupposupposupposuppos	erability va SE Emuct of Oraponent: 2 ponent: 2 ported verification of the protocolor of this rability of the protocolor of this rability of this rability of this rability of this rability of the protocolor of this rability of this protocolor of this rability of this protocolor of the protocolor of this protocolor of the protocolor of this protocolor of	nbedded acle Java 2D). rsions the re Java S ., 11.0.4 nbedded alt to exp allows acd attact access vecols to ava SE, J . Success	a SE nat EE: and d: oloit eker via	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
			cause service Java S Embe vulne Java of typical sandhat le untru that content Java s This vapply typical load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	chorized a partial se (partial se (partial se), Java Se deded. No rability a deployment of the cations of the c	I denial al DOS) SE ote: This applies the ents, fents run le (e.g., common the rely on the	of of of sto nning Start oxed SE 8), code the rity. es not nents, nat sted led CVSS				
N/A	16-10-2019	4.3	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). The supported version that is affected is 19.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise				https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			vulne Graal Edition significated addition Succes vulne unaution deletinates Oracle Edition CVSS (Integrates) Vector (CVSS	on. While rability in the control of	s in Orarprise as may mpact oducts. acks of t can resu creation odificati cal data M Enter sible dat Score 6 acts). C'	chis alt in a, on or all prise a. 5.8 VSS				
N/A	16-10-2019	4.3	Vulnes SE, Jar produ (compare af 7u23 13; Jar 8u22 vulne unaut with a multi compare attack vulne unaut cause service Java S	rability in a SE Employer of Orac onent: 2 or onent: 2	in the Janbedded acle Java 2D). The Java Strains the Java Strains allows access to ava SE, Java Strains access to ava SE, Java SE	va I I I I I I I I I I I I I I I I I I I	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			Java of typical sandhapplical fava and that lead that lead and the sandhapply typical load and code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	rability a leploymonally in clipoxed Java cations of applets (in a cations of a cations from the cations of a	ents, lents rur va Web S or sandb in Java S run le (e.g., c om the rely on t for secu ility doe deploym rvers, th only trus le install strator). e 3.7 mpacts) :N/AC:H C:N/I:N/	nning Start oxed EE 8), code the rity. es not nents, nat sted led CVSS				
N/A	16-10-2019	4	SE, Ja produ (composition production product	erability va SE En oct of Oraponent: oyment). Orted vered is Javentle Embedult to expendenticate ple protocomise Jabedded as requirection from than the	The rsion that a SE: 8u dded:	at is 221; 1221. Eker via Java sful n	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			vulne unaut insert some Embe as we read a Java S access vulne Java d typica sandb applic Java a that lo untru that c interr Java s This v apply typica load a code (by an 3.0 Ba (Conf Integr Vecto (CVSS N/UI:	essful attarability of thorized to delete of Java Sedded access to SE, Java Sedded attarability and polyeles (in oad and asted code omes from the Java of the Java	can result update, the access EE, Java Sincessible uthorized a subset EE Embera. Note: applies the ents, ents runule (e.g., com the rely on the rely o	It in It				
N/A	16-10-2019	4	SE pro SE (co Suppo are af 7u23:	erability in oduct of componer or ted verificated and and 1,8u221 ifficult to	Oracle J nt: Javad rsions th re Java S , 11.0.4	ava oc). nat E: and	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE.		
			Successful attacks require		
			human interaction from a		
			person other than the		
			attacker and while the		
			vulnerability is in Java SE,		
			attacks may significantly		
			impact additional		
			products. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Java SE accessible		
			data as well as		
			unauthorized read access		
			to a subset of Java SE		
			accessible data. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability does not		
			apply to Java deployments,		
			typically in servers, that		
			load and run only trusted		
			code (e.g., code installed		
			by an administrator). CVSS		
			3.0 Base Score 4.7		
			(Confidentiality and		

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
Weakness N/A	Publish Date 16-10-2019	4.3	Integral Vector (CVSS N/UI: CVE I Vulne SE, Jar produ (compose af 7u23 13; Jar 8u22 vulne unaut with multiple compose attack vulne unaut deleti acces Java Sacces vulne Java deleti acces vulne vuln	rity impa or: S:3.0/AV R/S:C/C D: CVE- erability va SE En act of Ora ponent: I orted ver fected an 1, 8u221 va SE En 1. Difficular thenticat network ple proto romise J nbedded as of this erability of thorized ion or most sto critical states and services and service	in the Janbedded acle Java Sanbedded attaces who cols to ava SE, Java Sances who cols to ava SE, Java Se	rSS I/PR: A:N). 999 va l a SE s). at E: and d: clarate sful lt in a, on or all dded This co	https://sty.netapy/advisorp-201910001/	securi p.com	A-NET-1 041119	E-SE-
			typica sandb applica Java a that le untru that co interr Java s This v be exp	deploymonally in clip oaxed Javantions of applets (in contract contract) and candbox in andbox in andbox in andbox in apploited by a specifie	ents rur va Web S r sandbe n Java S run e (e.g., com the rely on t for secur ility can y using	Start oxed E 8), code the rity.				
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	Publi	ish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				web s suppl CVSS (Integ Vector (CVSS N/UI	service values data 3.0 Base grity impor: S:3.0/AV:N/S:U/O	to the A e Score 5 pacts). C Z:N/AC:H C:N/I:H/	PIs. 5.9 VSS I/PR: (A:N).				
N/A		0-2019	4.3	SE, Ja produ (com Supp are at 7u23 13; Ja 8u22 vulne unau with multi comp SE Er attack unau cause service Java S Embe vulne Java of typice sandl appli Java at that I untru that of	va SE Er uct of Or ponent: orted ve ffected a 1, 8u221 va SE Er 1. Diffict rability thentica network ple prot oromise j nbedded ks of this erability thorized ca partia ce (parti SE, Java S edded. N erability deploym ally in cl poxed Ja cations o applets (oad and asted cod comes fr	rsions the re Java St., 11.0.4 mbedded alt to expend allows ted attack access to ocols to Java SE, ability the denial al DOS) SE ote: This applies tents, ients run va Web St. run de (e.g., ote., ote.)	a SE nat SE: and d: cloit cker via Java sful alt in co of of sto nning Start oxed SE 8), code	https://s ty.netapy /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	_
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	D	escription	& CVE II)	Pato	h	NCIIP	C ID
			This very be explicated in the Composition web supplicated (Available) (CVSS (CVSS N/UI:	andbox rulnerabeloited be specified onent, elevice which was about the specified onent, elevice which was about the specification of th	ility can y using d g, throu hich to the A Score 3 mpacts)	also APIs igh a PIs. .7 /PR: A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Concurversion are Ja 11.0.4 Ember Unaut with I multiple comp SE En attack vulne unaut cause service Java S Ember Vulne explodata t specification of the speci	rability in a SE Employ on SE Employ on SE: 70 and 13; dded: 80 and 13; dded: 80 and 14 and 15 and 1	support are affect at 231, 80 at 221. The allows access we cols to ava SE, J. Success ability the all DOS) of E an only upplying the ponent	ker ria ava sful lt in of of be	https://ty.netap/advisorp-20191	p.com ry/nta	A-NET-1 041119	
CV Scoring Scal	le 0-1	1-2	2-3	8				7-8		

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			appli Java a throu CVSS (Avai CVSS (CVSS N/UI	applets, sigh a we 3.0 Base lability i Vector: 5:3.0/AV	or Untrusuch as b service Score 3 mpacts) Z:N/AC:HC:N/I:N/	e. 3.7 I/PR: 'A:L). 964				
	16-10-2019	4.3	SE, Ja produ (com Supp are at 7u23 13; Ja 8u22 vulne unau with multi comp SE Er attack unau cause service Java S Embe vulne Java at tack unau typica sandli appli Java at that luntru	va SE Eract of Orponent: orted ve ffected a 1, 8u221 va SE Eract of Originality thentical metwork ple protoromise of complete (particle) feet	rsions the re Java St., 11.0.4 mbedded alt to expend allows ted attack access to cools to Java SE, ability the denial al DOS) SE ote: This applies the ents, ients run va Web Strun de (e.g., ote gas, ote gas, ote sandbox and box sandbox sa	a SE nat SE: and d: cloit cker via Java sful ult in co of sto nning Start oxed SE 8),	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			Java some the composition of the	net) and sandbox vulnerabe ploited be specified be specified and a service where the	for seculity can by using and age, through the A secure 3 mpacts)	rity. also APIs ugh a PIs. 3.7 . I/PR:				
N/A	16-10-2019	5.8	SE, Ja produ (com Suppare at 8u22 SE En Diffic vulne unaut with a multi compate some Emberand uto causervice Java SE Emberand	erability va SE En orted ve fected a 1, 11.0.4 hbedded ult to ex rability thenticat network ple prote romise J hbedded to of Java S edded ac nauthor use a par ce (parti- ce (parti- ce) chaded. N orability	nbedded acle Java Scripting rsions the result of the second state of the second state of the second	d sE g). nat SE: Java	https://s ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET-1 041119	
	<u> </u>		l						I	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L).		
			CVE ID : CVE-2019-2975		
e-series_sant	tricity_storage	_manaį			
N/A	16-10-2019	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/416

0-1

CV Scoring Scale

4-5

3-4

2-3

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			other Succes vulne unaut cause service Java S Embe vulne Java of typical sandhapplice Java sandhapplice Java sandhapplice interregion Java sandhapplice interregion Java sandhapply typical sandhapply typical load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	than the essful attrability of thorized a partial at Equation (Equations of the estimated and ested code administration (e.g., co	e attacker acks of the can result ability to ability to ability to ability to a sandboard and	er. chis chis chis clt in co of of sto nning Start oxed SE 8), code the rity. es not nents, nat sted led CVSS . I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Ja produ (composuppe are af 7u23 13; Ja 8u22	erability va SE En oct of Ora ponent: l orted ver fected an 1, 8u221 va SE En 1. Difficu	nbedded acle Java Kerbero rsions thre Java S ., 11.0.4 nbedded	l a SE s). nat SE: and l:	https://sty.netapy/advisorp-201910001/	p.com y/nta	A-NET- 041119	
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

unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSSS:3.0/AV:N/AC:H/PR: N/UI:N/S:C/C:H/I:N/A:N). CVE ID: CVE-2019-2949 N/A 16-10-2019 5.8 Vulnerability in the Java https://securi	Weakness	Publish Date	CVSS	D	escription	& CVE I	D	Pato	h	NCIIP	CID
This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:C/C:H/I:N/A:N). CVE ID: CVE-2019-2949 N/A 16-10-2019 5.8 Vulnerability in the Java https://securi	Weakness	Publish Date	CVSS	unaut with a Kerbe Java S Embe vulne Java S addit Succes SE Endata. vulne Java of typica sandkapplic Java a that kerbe untrue that of internal sandkapplic sandkapplic Java a that kerbe untrue that of internal sandkapplic sandkapplic Java a that kerbe untrue that of internal sandkapplic sandkap	thenticate network eros to comes from the comes fro	red attace access to access to thile the sin Java dded, at attly impoducts. access to	eker via nise a SE, tacks act chis clt in co ete ava ble co nning Start oxed SE 8), code	Patc	:h	NCIIP	CID
N/UI:N/S:C/C:H/I:N/A:N). CVE ID : CVE-2019-2949 N/A 16-10-2019 5.8 Vulnerability in the Java https://securi				that control interregions of the extended of t	comes fromet) and sandbox wilnerabe ploited be specified onent, endies data and 3.0 Base didentiali Vector:	om the rely on for secuility can y using defich to the A Score 6 ty imparts	the rity. also APIs ugh a PIs. .8 cts).				
TATION TO THE TATION THE TATION TO THE TATION TO THE TATION TO THE TATION TO THE TATIO	N/A	16-10-2019	5.8	N/UI:N/S:C/C:H/I:N/A:N). CVE ID: CVE-2019-2949 Vulnerability in the Java				https://s	securi	A_NET_	 F_CF_
SE product of Oracle Java ty.netapp.com	CV Scoring Sca			SE product of Oracle Java							9-10

Weakness	Publish Date	CVSS	Descriptio	n & CVE II)	Patc	h	NCIIP	C ID
			SE (compone	nt: Hotsp	ot).	/advisor	y/nta	041119	/418
			Supported ve	rsions th	at	p-20191	017-		
			are affected a	re Java S	E:	0001/			
			11.0.4 and 13	B. Difficul	t to				
			exploit vulne	rability					
			allows unaut	henticate	ed				
			attacker with	network	ζ				
			access via mu	ıltiple					
			protocols to o	comprom	ise				
			Java SE. Succe	essful att	acks				
			of this vulner	ability ca	an				
			result in unau	uthorized	l				
			read access to	o a subse	t of				
			Java SE acces	sible data	a				
			and unauthor						
			to cause a pai		-				
			service (parti						
			Java SE. Note	_					
			yulnerability		0				
			Java deploym						
			typically in cl		ning				
			sandboxed Ja		_				
			applications						
			Java applets (
			that load and	•	,,				
			untrusted cod		ode				
			that comes fr		ouc				
			internet) and		-he				
			Java sandbox	-					
			This vulneral						
			apply to Java	_					
			typically in se						
			load and run	-					
			code (e.g., cod						
			by an admini	_	CV32				
			3.0 Base Scor						
			(Confidential	-	OT TOO				
			Availability in	npacts).	CVSS				
			Vector:						
			(CVSS:3.0/AV	•	•				
			N/UI:N/S:U/	C:L/I:N/A	A:L).				
CV Scoring Sca									

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2977		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/419
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	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
Weakness N/A	Publish Date 16-10-2019	4.3	(Available (CVSS) N/UI: CVE I Vulne SE, Ja produ (composuppe are aff 7u23 13; Ja 8u22 vulne unaut with multi composE En attack vulne unaut cause	escription lability in Vector: 5:3.0/AV N/S:U/O D: CVE- rability in rability in the content of Ora ponent: J orted ven fected an 1, 8u221 va SE En 1. Difficult rability in the proto romise J inbedded is of this rability of chorized a partial te (partial	mpacts) :N/AC:H ::N/I:N/ 2019-2 in the Ja nbedded acle Java AXP). rsions the re Java S , 11.0.4 nbedded access where allows red attack access where access wher	I/PR: A:L). 978 Iva I SE and I: bloit cker via ava sful alt in co of	https://s ty.netap /advisor p-20191	securi p.com	A-NET-1 041119	E-SE-
			Java S Ember vulne Java of typica sande applica Java a that le untru that of interr Java s This w be exp	ce (partial E, Java S edded. No rability a leployme ally in clipoxed Java ations of a leplets (in sted codes from and box and box and box a lepleted be specifie	E ote: This applies tents, ents rur va Web S r sandb n Java S run e (e.g., com the rely on to for secu- ility can y using	stoonning Start oxed EE 8), code the rity.	0001/			
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	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			web s suppl CVSS (Avai CVSS (CVSS N/UI:	service we ies data 3.0 Base lability in Vector: S:3.0/AV N/S:U/C	thich to the A Score 3 mpacts) :N/AC:H ::N/I:N/	PIs. .7 I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Ja produ (comp Serial version are Ja 11.0.4 Ember Unit of the comp SE En attack vulner unaut cause service Java Service sandk applied Java attack untru	erability a va SE Em act of Ora ponent: dization). In that a va SE: 70 and 13 and 13 and all to expended a partial of the protographic of this rability of the protographic apartial of the pr	Supportare affect 1231, 80 access who cols to ava SE, Java SE ava SE, Java Sents rura Web Sents, ents rura Web Sents, ents rura Web Sents, ents rura wa	ted ted ted 1221, ker via lava sful lt in o of of of start oxed E 8),	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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	D	escription	a & CVE II	D	Pato	:h	NCIIP	C ID
			Java so This was the explication of the Composite of the CVSS (Available) (CVSS (CVSS N/UI:	net) and andbox rulnerab ploited b specifie onent, e ervice w ies data 3.0 Base lability in Vector: 5:3.0/AV N/S:U/C D: CVE-	for secuility can y using deg., throughich to the A Score 3 mpacts)	rity. also APIs ugh a PIs7 . (/PR: A:L).				
N/A	16-10-2019	4.3	SE prosections SE (consumption of SE (consumption o	rability oduct of omponer orted verifected and 13 it vulner is unauth it ser with its via multiple of services of Java Strability and leploymed lay in clipoxed Java Strability and ones fromes from the	Oracle Jat: 2D). It is a particular ability can be a parti	ava at E: t to ed c acks an d ial ial ial This co aning Start oxed E 8),	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET-1 041119	
CV Scoring Sca	le 0-1	1-2	2-3	Locy and	2019 011					

Weakness	Publish	Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
				This very be explicated by the explication of the composition of the c	andbox vulnerab ploited b e specific conent, e ervice w ies data 3.0 Base lability i Vector: 6:3.0/AV N/S:U/O	oility can by using ed e.g., throw which to the A e Score 3 mpacts)	also APIs ugh a PIs. .7 I/PR: A:L).				
N/A	16-10-2	2019	4.3	Vulnes SE, Jar produ (comp Suppor are aff 7u23: 13; Ja 8u22: vulnes unaut with a multi comp SE Emattack vulnes unaut cause service Java SE Ember vulnes Java	erability va SE En oct of Or ponent: orted ve fected a 1, 8u221 va SE En 1. Difficu rability chentical network ple prote romise J nbedded as of this rability chorized a partia ce (parti SE, Java Se edded. N rability leploym ally in cla oxed Jav cations of pplets (in the Janbedded acle Java 2D). rsions the re Java St., 11.0.4 mbedded all to expall t	ava I I I I I I I I I I I I I I I I I I	https://s ty.netapy /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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	D	escription	ı & CVE II	D	Pato	:h	NCIIP	C ID
			untru that c interr Java s This v apply typica load a code (by an 3.0 Ba (Avail CVSS (CVSS N/UI:	S:3.0/AV N/S:U/C	le (e.g., com the rely on the for securility doe deploymers, the only trusted install etrator). eta 3.7 mpacts). eta N/AC:H	the rity. es not nents, nat sted ed CVSS				
N/A	16-10-2019	4.3	Vulne Graal' Java). versic 19.2.0 vulne unaut with r multip comp Graal' Edition vulne Graal' Edition significand succe	multiple protocols to compromise Oracle GraalVM Enterprise		https://sty.netapy/advisorp-20191	p.com ry/nta	A-NET-1 041119		
			acces	s to critic		or all				

Weakness	Publish Date	CVSS	D	escription	ı & CVE II	D	Pato	h	NCIIP	C ID
			Edition CVSS (Integrated Vector (CVSS N/UI: CVE I	6:3.0/AV N/S:C/C D : CVE - erability	sible dat Score 6 acts). C' :N/AC:H :N/I:H/ 2019-2 in the Ja	a. .8 VSS I/PR: A:N). 989 va				
N/A	16-10-2019	4.3	produ (com) Suppo are af 7u23 13; Ja 8u22 vulne unaut with in multi comp SE En attack vulne unaut cause service Java S Embe vulne Java o typica sandk applie Java a that le untru that c intern	va SE Emuct of Oraponent: 2 ponent: 2 ponent: 2 ported verificated and a partial cally in clipoxed Java SE dded. No rability a leploymouth of the poxed Java Se dded. No rability a leploymouth of the poxed Java Se (partial poxed J	acle Java 2D). rsions the re Java S , 11.0.4 hbedded alto expend access we can resurability to denial ald DOS) of the resurable strong and Serva Web Serva W	asE at E: and d: bloit ker via ava sful lt in o of of of start oxed E 8),	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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	D	escriptio	tion & CVE ID		Pato	h	NCIIP	C ID
			apply typical load a code by an 3.0 B (Avai CVSS (CVSS	vulnerable to Java ally in seand run (e.g., cool administrates Scorlability in Vector: S:3.0/AV:N/S:U/O:CVE	deploynervers, the only true de installestrator). e 3.7 mpacts) Z:N/AC:HC:N/I:N/	nents, nat sted led CVSS . I/PR:				
N/A	16-10-2019	4	SE, Ja production of the support of the succession of the support	erability va SE Er ponent: pyment) orted ve ded is Jav SE Embe ult to ex erability thentica network ple prot promise than the erability thorized t or dele of Java S edded ac ell as una access to SE, Java S sible dat erability	nbedded acle Java The rsion that a SE: 8u dded: 8u ploit allows ted attacks of the care success of the car	at is 221; u221. Cker via Java sful n rson er. Chis ult in SE data ed et of edded This	https://s ty.netapy /advisor p-20191 0001/	p.com y/nta	A-NET-1 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			typical sandbapplical sandbapplical formula interrope and a sandbapply typical load a code by an 3.0 Bac (Confintegration (CVSS N/UI:	deploymentally in clipoxed Javanders (in comes from and box in the Javanders (e.g., cod administic ase Score (identiali rity imparts (E:3.0/AV R/S:U/C D: CVE-	ents runva Web Sor sandbin Java Sor un le (e.g., com the rely on the for secuility does deploymers, the only trus le install strator). Le 4.2 ty and lects). CV	Start oxed E 8), code the rity. es not nents, at sted ed CVSS				
N/A	16-10-2019	4	SE prosections SE (constructions SE (constructions) Successive Suc	erability oduct of omponer orted verificated and the rability at the protocomise Jessful attains on other the rability is may since may	Oracle Javad rsions the Java St., 11.0.4 of exploit allows access vaccess vaccess vaccess required than the while the is in Java	ava oc). nat E: and eker via uire om a e	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escription	a & CVE II	D	Pato	h	NCIIP	CID
			impace production attack vulne unaut insert some data a unaut to a single applied appl	ct addition acts. Such as of this rability of thorized of Java Sas well as chorized abset of actions of polets (in actions of polets)).	can resurupdate, can resurupdate, ce access read access run resurup run	It in s to sible cess This co nning Start oxed E 8), code the rity. cs not nents, at sted ed CVSS				
			CVE I	D : CVE-	2019-2	999				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE:				securi p.com ry/nta .017-	A-NET- 041119	
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	D	escription	a & CVE II	D	Pato	h	NCIIP	CID
Weakness	Publish Date	CVSS	7u23: 13; Ja 8u22: vulne unaut with in multi comp SE En attack vulne unaut deleti acces: Java S acces: vulne Java d typica sandb applic Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Integ Vecto	1, 8u221 va SE En 1. Difficult rability a chenticate network ple proto romise Ja nbedded as of this rability a chorized on or mo s to critic se, Java S sible dat rability a deployme ally in cli boxed Jav cations o applets (i oad and i oad and i oat and cations o applets (i oad and i oxed Jav cations o applets (i oad and i oxed Jav cations o applets (i oad and i oxed Jav cations o applets (i oad and i oxed Jav cations o applets (i oad and i oxed Jav cations o applets (i oad and i oxed Jav cations o applets (i oad and i oxed Jav cations o applets (i oxed Jav cations o app	to expallows ed attack access who cols to ava SE, J. Success can resurce attack attack at the ents, ents run e (e.g., com the rely on the	and l: loloit ker via ava sful lt in or all dded This to aning Start oxed E 8), ode the rity. also APIs also APIs Igh a PIs9	Patc	ch .	NCIIP	CID
			-	N/S:U/C D : CVE-		-				
N/A	16-10-2019	4.3	Vulne	erability in the second	in the Ja	va	https://s		A-NET-	E-SE-
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
			product of Oracle Java SE	/advisory/nta	041119/429
			(component: 2D).	p-20191017-	
			Supported versions that	0001/	
			are affected are Java SE:		
			7u231, 8u221, 11.0.4 and		
			13; Java SE Embedded:		
			8u221. Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized ability to		
			cause a partial denial of		
			service (partial DOS) of		
			Java SE, Java SE		
			Embedded. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability can also		
			be exploited by using APIs		
			in the specified		
			Component, e.g., through a		
			web service which		
			supplies data to the APIs.		
			CVSS 3.0 Base Score 3.7		
			(Availability impacts).		
			CVSS Vector:		
			(CVSS:3.0/AV:N/AC:H/PR:		
			(CV33.3.0/AV.IV/AC:IT/PK:		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N/UI:N/S:U/C:N/I:N/A:L).		
			CVE ID : CVE-2019-2962		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2964	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/430
					1

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts).	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/431

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2973 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit
SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221.
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
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
			This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L). CVE ID: CVE-2019-2975		
e-series_sant	tricity_unified_	manag	ger		
N/A	16-10-2019	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments,	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/433

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			sandbapplications application interresponding that is untrued that continued interresponding to the second of the second is untrued that continued interresponding typication is untrued to the second of the second interresponding typication is untrued to the second interresponding typication in the second interresponding typication is untrued to the second interresponding typication is untrued to the second interrespond typication is untrued to the second interresponding typication	ally in clipoxed Javantions of applets (in pad and sted code administ ase Score ability in Vector: 8:3.0/AV R/S:U/OD: CVE-	va Web Sor sandbox san	Start oxed oxed (E 8), code the rity. es not nents, nat sted cVSS . I/PR: A:L).				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with r Kerbe Java S Embe vulne Java S additi	rability va SE Em orted verse fected and fected and fected and SE Em orthogonal prosessful attached and prosesful attached and prosesful attached attached and prosesful attached attached attached and prosesful attached	in the Janbedded acle Java Scribero Scr	va l s SE s). nat EE: and d: oloit eker via nise	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			unaut critical access. SE Endata. vulne Java de typical sandband applied Java at that le untrue that content Java so This volume be explied to the Composite of the Composite of the Composite of the Composite of the CVSS (CVSS (CVSS N/UI:		access to recompliance SE, Jaccessil accessil accessil ais applies to ents, itents run le (e.g., com the rely on for secundility can be secundility.	to ete ava ble to ming Start oxed EE 8), code the rity. also APIs ugh a PIs. a.8 cts).				
N/A	16-10-2019	5.8	N/UI:N/S:C/C:H/I:N/A:N). CVE ID: CVE-2019-2949 Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks				https://s ty.netapy /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIF	C ID
			of this result read a Java S and us to cause service Java S vulner Java d typica sandb applice Java a that le untru that cointern Java s This vapply typical load a code (by an 3.0 Ba (Confi Availa Vecto (CVSS N/UI:	s vulneration unautaccess to E access nauthorings a partice (partialized land particular and land land land land land land land	ability can thorized a subset ized abilitied abilitial denied abilitial denied and DOS) of This applies to ents run are (e.g., common the rely on the	an d et of a lity ial of of to nning Start oxed EE 8), code the rity. es not nents, nat sted led CVSS I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Jav produ (comp Suppo are af 7u232 13; Ja	erability in a SE Emuct of Oraconent: Norted verificated and 1, 8u221 va SE Endander.	nbedded acle Java Network rsions th re Java S , 11.0.4 nbedded	l a SE king). nat SE: and l:	https://sty.netapy/advisorp-201910001/	p.com y/nta	A-NET- 041119	

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	:h	NCIIF	CID
Weakness	Publish Date	CVSS	vulne unaut with r multip comp SE En attack vulne unaut cause servic Java S Embe vulne Java d typica sandb applic Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (Avail CVSS N/UI: Vulne	rability and henticate protocomise John bedded as of this rability and apartiance (partially in clipated and sted code omes from the poloited by specified and box and	allows access to access to access to ava SE, J . Success can resu ability t I denial al DOS) access car resu ability t I denial al DOS) access car resu ability t I denial al DOS) access car resu ability t I denial al DOS) access car resu ability t I denial al DOS) access car resu ability t and access applies t access acces	eker via lava sful lt in to of of lava start oxed let 8), lava start oxed let 8), lava lava lava lava lava lava lava lav			NCIIF	PCID
N/A	16-10-2019	4.3	SE, Ja produ (com	va SE En act of Ora conent: J orted ver	nbedded acle Java [AXP].	l a SE	https://securi ty.netapp.com /advisory/nta p-20191017-			
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
			are affected are Java SE:	0001/	
			7u231, 8u221, 11.0.4 and		
			13; Java SE Embedded:		
			8u221. Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized ability to		
			cause a partial denial of		
			service (partial DOS) of		
			Java SE, Java SE		
			Embedded. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability can also		
			be exploited by using APIs		
			in the specified		
			Component, e.g., through a		
			web service which		
			supplies data to the APIs.		
			CVSS 3.0 Base Score 3.7		
			(Availability impacts).		
			CVSS Vector:		
			(CVSS:3.0/AV:N/AC:H/PR:		
			N/UI:N/S:U/C:N/I:N/A:L).		
			CVE ID : CVE-2019-2981		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/438

Weakness	Publish Date	cvss	D	escription	ı & CVE II	D	Pato	h	NCIIP	C ID
Weakness N/A	Publish Date	4.3	(Available	escription lability in Vector: S:3.0/AV N/S:U/O D: CVE- erability: oduct of omponer orted ven fected and 13. it vulner s unauth s via mult cols to co SE. Succe s vulnera it in unau y to caus l of servi of Java S rability a	mpacts) :N/AC:H ::N/I:N/ 2019-2 in the Ja Oracle J nt: 2D). rsions the re Java S : Difficult rability renticate metworl ltiple omprone ssful att ability ca thorized e a part ice (part E. Note:	I/PR: A:L). 983 Iva ava att EE: at to ed k acks an d ial tial tial	https://ty.netap	securi p.com	A-NET-	
			typical sandbapplical sandbapp	leploymonally in clipoxed Javantions of applets (in oad and oat and box and bo	ents rur ya Web S r sandb in Java S run le (e.g., c om the rely on t for secu ility can by using d l.g., throu which to the A Score 3	Start oxed SE 8), code the rity. APIs ugh a PIs.	p-20191 0001/		041119	/439
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

CVSS Vector: (CVSS:3.0/AV:N/AG N/UI:N/S:U/C:N/I: CVE ID : CVE-2019 Vulnerability in the SE, Java SE Embedo product of Oracle Ja	e Java ded	
SE, Java SE Embedo product of Oracle Ja	ded	
(component: 2D). Supported versions are affected are Jav 7u231, 8u221, 11.0 13; Java SE Embedde 8u221. Difficult to evulnerability allow unauthenticated at with network access multiple protocols compromise Java S SE Embedded. Succe attacks of this vulnerability can reunauthorized ability cause a partial deniservice (partial DO) Java SE, Java SE Embedded. Note: T vulnerability applied Java deployments, typically in clients of sandboxed Java We applications or sand Java applets (in Java that load and run untrusted code (e.g. that comes from the internet) and rely company to Java deployers. This vulnerability of apply to Java deployers, typically in servers, load and run only to servers.	va SE: 0.4 and ded: exploit vs ttacker ss via to EE, Java cessful esult in ty to ial of S) of Only This es to running eb Start adboxed va SE 8), g., code ae on the ecurity. does not syments, s, that	A-NET-E-SE- 041119/440
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5		8-9 9-10

code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS.3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988 Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). The supported version that is affected is 19.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data. CVSS 3.0 Base Score 6.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:C/C:N/I:H/A:N). CVE ID: CVE-2019-2989	Weakness	Publish Date	cvss	Descriptio	n & CVE ID	Pato	h	NCIIP	CID
GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). The supported version that is affected is 19.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data. CVSS 3.0 Base Score 6.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:C/C:N/I:H/A:N).				by an administ 3.0 Base Scor (Availability in CVSS Vector: (CVSS:3.0/AV N/UI:N/S:U/CCVE ID : CVE	strator). CVSS e 3.7 mpacts). ':N/AC:H/PR: C:N/I:N/A:L). -2019-2988				
	N/A	16-10-2019	4.3	GraalVM Enteredition production of that is 19.2.0. Difficult vulnerability unauthentical with network multiple protuble compromise of GraalVM Enteredition. While vulnerability GraalVM Enteredition, attack significantly is additional producted for a compromise of GraalVM enteredition, attack significantly is additional producted for a compromise of GraalVM enteredition or maccess for critical or access to critical or access to critical for a compromise of GraalVM enteredition or maccess to critical for a compromise of GraalVM enteredition or maccess to critical for access to critical for access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition access to CVSS 3.0 Base (Integrity improved the compromise of GraalVM enteredition	erprise act of Oracle apponent: oported s affected is alt to exploit allows ted attacker access via ocols to Oracle erprise e the is in Oracle erprise ks may mpact oducts. cacks of this can result in creation, odification cal data or all M Enterprise sible data. e Score 6.8 oacts). CVSS	ty.netapy /advisor p-20191	p.com y/nta		

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts).	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/442

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
			(CVSS N/UI:	Vector: 5:3.0/AV N/S:U/C D : CVE-	:N/I:N/	A:L).				
N/A	16-10-2019	4	Vulne SE, Jar produ (composition production	erability in a SE Emple of Java SE Embedded as required than the essful attained as reability of Java SE Embedded as required than the essful attained as the essful attained and essful as the essful attained and essful as the essful attained and essful as the essful attained and essful attained as the essful attained as	in the Janbedded acle Java The resion that a SE: 8u dded: 8u ploit allows red attacked access to ava SE, Java Se attacked acks of the can resulupdate, a subset as who is a subset as w	va lasE at is 221; 1221. eker via (ava sful n eson er. chis lt in sto SE data ed et of dded This co nning Start oxed E 8),	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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 Da	te CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
			Java s This v apply typica load a code by an 3.0 Ba (Conf Integr Vecto (CVSS	net) and candbox vulnerable to Java ally in send run (e.g., cocadministic ase Score identialistic imparts.	for secupility does deploymervers, the only trusted install strator). The equation of the equa	rity. es not nents, nat sted led CVSS				
N/A	16-10-201	9 4	Vulnes SE prosection SE (construction SE	erability oduct of omponer orted verability of fected a 1, 8u221 of fiftigult to the orthogonal of the	in the Ja Coracle J Int: Javad rsions the re Java S L, 11.0.4 D exploit allows ted attact access to cacks rece ction fro than the while the is in Java ignificar onal cessful can resu update, te access EE acces	va ava loc). nat SE: and eker via quire om a e a SE, ntly	https://s ty.netapy /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			to a single accession vulner accession vulner accession vulner accession vulner accession version vers	chorized ubset of sible data rability a leployme ally in clipoxed Java cations of sted code and sted code and so Java cally in second run of le.g., code administic ity imparts: S:3.0/AVR/S:C/C	Java SE a. Note: applies ents, ents run va Web or sandb in Java S run le (e.g., o om the rely on for secu deployn rvers, th only tru le instal strator). e 4.7 ty and acts). CV	This to nning Start loxed SE 8), code the arity. es not nents, nat sted led CVSS				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with i multi	erability va SE En oct of Ora ponent: l orted ver fected an 1, 8u221 va SE En 1. Difficu rability a chenticat network ple proto romise J	nbedded acle Java Librarie rsions the re Java S ., 11.0.4 mbedded alt to exp allows ted attac access	d SE es). hat SE: and d: ploit cker	https://sty.netapy/advisorp-20191	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIF	CID
weakness	Publish Date	CV3S	SE En attack vulne unaut deleti acces. Java S acces vulne Java deleti application of typical sandk application of the control of the experience of the composition of	abedded as of this rability of chorized on or more as to critical and in the control of the cont	can result creation odification odification odification odification odification of the can be supplied of the can	sful alt in an, on or all edded This to nning Start oxed SE 8), code the rity. also APIs ugh a PIs. 5.9 VSS I/PR: (A:N).	Patc		NCIIP	
N/A	16-10-2019	4.3	SE, Ja produ (composuppe are af 7u23 13; Ja 8u22	erability va SE En oct of Ora ponent: 2 orted ver fected an 1, 8u221 va SE En 1. Difficu	nbedded acle Java 2D). rsions the re Java S ., 11.0.4 nbedded	l a SE nat SE: and l:	https://sty.netapy/advisorp-201910001/	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
Weakness	Publish Date	CVSS	unaut with a multiple composed service service sands applied Java at that left untrue that control interrol Java service sands applied Java at that left untrue that control interrol Java service service sands applied Java at that left untrue that control interrol Java service service service sands applied Java at that left untrue that control interrol Java service	escription chenticate network ple prote romise J nbedded as of this rability of chorized a partia E, Java S dded. No rability a leployme ally in cli poxed Jav cations of pplets (i pad and sted cod omes fro net) and randbox i vulnerab ploited b especifie conent, e service w	ted attack access we be cols to ava SE, Jones ability to a le	cker via lava sful lt in o of of sto nning Start oxed E 8), code the rity. also APIs	Pato	ch .	NCIIP	PC ID
			web s suppl CVSS (Avail CVSS (CVSS N/UI:	ervice wies data 3.0 Base lability in Vector: 5:3.0/AV N/S:U/C	which to the A Score 3 mpacts) :N/AC:H	PIs. .7 I/PR: A:L).				
			Vulne SE, Ja	D: CVE- erability: va SE Em ict of Ora	in the Ja	va l	https:// ty.netap	p.com	A-NET-	E-SE-
N/A	16-10-2019	4.3	(comp	ponent: urrency) ons that	. Suppoi	ted	/advisor p-20191 0001/		041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			11.0.4 Ember Diffict vulne unaut with a multiple comp SE En attack vulne unaut cause service Java S Ember vulne explodata t specific without Java V applied Java a throut CVSS (Availa CVSS (CVSS N/UI:	va SE: 70 dand 13 dded: 80 ult to exp rability a chenticate network ple proto romise J nbedded as of this rability a chorized a partia a partia a partia a partia be (partia a partia a partia be (partia a partia be (partia a partia be (partia a partia be (partia a partia a partia be (p	g Java SE 1221. ploit allows red attace access wo cols to ava SE, J resurs ability to denial all DOS) of the ponent to the ponent to the ponent to service access wo service access an access access to service access acce	ker ria ava sful lt in o of of seed sted e7 I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppo are af 7u23: 13; Ja	rability va SE En oct of Ora conent: J orted ver fected ar 1, 8u221 va SE En 1. Difficu	nbedded acle Java (AXP). rsions th re Java S , 11.0.4 nbedded	SE nat E: and	https://sty.netapy/advisorp-20191	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE I	D	Pato	ch	NCIIF	C ID
Weakness	Publish Date	CVSS	vulne unaut with in multiple composed service Java S Ember vulne Composed S Ember vulne S	rability and hetwork ple protections of this rability and and sted code	allows add attack access of access of access of ava SE, Jones and addity to the all DOS) of applies to ents run ability to the series applies to ents run be (e.g., company using of access) and all to the Access of ac	cker via Java sful It in to of of sto nning Start oxed EE 8), code the rity. also APIs ugh a PIs. 5.7 . J/PR: GA:L).	Pato	ch	NCIIF	PCID
N/A	16-10-2019	5.8	SE, Ja produ (com	erability of the second	nbedded acle Java Scripting	l a SE g).	https:// ty.netap /advisor p-20191	p.com ry/nta	Marka A-NET-E-SE- ta 041119/449	
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
			are affected are Java SE:	0001/	
			8u221, 11.0.4 and 13; Java		
			SE Embedded: 8u221.		
			Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Java SE, Java SE		
			Embedded accessible data		
			and unauthorized ability		
			to cause a partial denial of		
			service (partial DOS) of		
			Java SE, Java SE		
			Embedded. Note: This		
			vulnerability applies to		
			* * * *		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability can also		
			be exploited by using APIs		
			in the specified		
			Component, e.g., through a		
			web service which		
			supplies data to the APIs.		
			CVSS 3.0 Base Score 4.8		
			(Integrity and Availability		
			impacts). CVSS Vector:		

Weakness	Publish Date CVSS Description & CVE ID		Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:H/PR:		
			N/UI:N/S:U/C:N/I:L/A:L).		
			CVE ID : CVE-2019-2975		
e-series_san	tricity_web_sei	rvices_	proxy		
N/A	16-10-2019	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-E-SE- 041119/450

Weakness	Publish Date	cvss	D	escription	ո & CVE II	0	Patc	h	NCIIP	C ID
			apply typica load a code (by an 3.0 Ba (Avail CVSS (CVSS N/UI:	vulneraby to Java of ally in second (e.g., cod administ ase Score lability in Vector: S:3.0/AV R/S:U/C	deploymervers, the constall strator). e 3.1 mpacts). :N/AC:H	nents, nat sted ed CVSS I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with a Kerbe Java S Embe vulne Java S additi Succe vulne unaut critica access SE En data. I vulne Java d	erability in va SE Emponent: It ponent: It p	nbedded acle Java Kerberon rsions the re Java S ., 11.0.4 nbedded all to exp allows access v omprom SE Thile the is in Java dded, att actly impa oducts. acks of t can resu access t r comple ava SE, Ja accessil ais applies t ents,	s). a SE s). at EE: and d: bloit eker via aise a SE, tacks act chis lt in o ete ava ble	https://s ty.netapj /advisor p-20191 0001/	p.com ry/nta	A-NET-1 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			application Java a that lead that continued in the Composition of the Composition of the Composition of the Composition of the CVSS (CONFICT CVSS (CVSS N/UI:	cations of applets (in pad and and sted code and	or sandb in Java S run le (e.g., com the rely on a for secu ility can by using d .g., through thich to the A Score 6 ty impa	oxed SE 8), code the rity. also APIs ugh a PIs. 5.8 cts).				
			SE prosection SE (constraints of Supposer and 11.0.4) exploallow	erability oduct of omponer orted verificated and 13 it vulner sunauth	Oracle J nt: Hotsp rsions th re Java S Difficul rability nenticate	ava pot). nat SE: It to				
N/A	16-10-2019	5.8	access proto Java S of this result read a Java S and u to cau service Java S	ser with s via mulcols to cols to cols to cols to cols in unauticess to E access nauthor ise a partice (partice). Note: rability a	ltiple ompron ssful att ability ca thorized a subse sible dat ized abi tial deni al DOS) This	nise cacks an d et of a lity ial of	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET-1	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			typical sandbapplical sandbapplical sandbapplical sandbapplical sandbapply typical sandbapply typical sandbapply typical sandbapply typical sandbapply typical sandbapply sandba	leploymed ally in clipoxed Javacations of applets (in steed code omes from the andbox from the Javacation of the Javacat	ents runya Web Sar sandban Java Sarun he (e.g., com the rely on the for secuality does deploymervers, the only truste install trator). Et 4.8 ty and he pacts).	Start oxed oxed EE 8), code the rity. es not nents, nat sted ed CVSS CVSS I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Japrodu (comp Suppo are af 7u23; Ja 8u22; vulne unaut with multicomp SE En attack vulne	erability in va SE Emponent: It of Oraponent: It or of Oraponent: It or of Oraponent: It or of Oraponent It	nbedded acle Java Network rsions the Java Strate Java Strate allows access vaccess vacces vacc	I a SE king). nat SE: and d: oloit ker via Java sful	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE I	D	Pato	h	NCIIP	CID
			service Java S Ember Vulne Java d typica sandh applice Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	a partia ce (partia ce (partia ce), Java S dded. No rability a leployme ally in cli boxed Jav cations o applets (i boad and sted cod andbox vulnerab ploited b especifie conent, e ervice w ies data 3.0 Base lability in Vector: 6:3.0/AV N/S:U/C D: CVE-	al DOS) SE ote: This applies ents, ients run le (e.g., o om the rely on for secu oility car oy using ed .g., thro which to the A e Score 3 mpacts)	of sto nning Start oxed SE 8), code the rity. also APIs ugh a .PIs. 3.7 . H/PR: 'A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with i multij	erability va SE En oct of Ora ponent: J orted ver fected an 1, 8u221 va SE En 1. Difficu rability a chenticat network ple proto romise J	nbeddedacle Java JAXP). rsions the re Java S ., 11.0.4 mbedded alt to exp allows ted attact access to	d SE nat SE: and d: oloit cker via	https://sty.netapy/advisorp-20191	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
			SE En attack vulne unaut cause service Java S Embe vulne Java of typica sandk applie Java athat kuntru that cointern Java s This voice expire the Composite of typical sandk applie Java athat known that cointern Java s This voice expire the Composite of typical sandk applie (CVSS (Avail CVSS (CVSS N/UI:	nbedded as of this crability of thorized a partial ace (partial ace (p	can result ability to ability to the Action of the Action	sful sful alt in co of of sto nning Start oxed SE 8), code the rity. also APIs ugh a PIs. 3.7 . I/PR: (A:L).				
N/A	16-10-2019	4.3	SE, Ja produ (comp Serial version are Ja 11.0.4 Embe	erability va SE En uct of Ora ponent: lization). ons that a va SE: 70 4 and 13 edded: 80 ult to ex	nbedded acle Java . Suppor are affec u231, 8u ; Java SE u221.	ted cted 1221,	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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	D	escription	a & CVE I	D	Pate	ch	NCIIF	C ID
Weakness	Publish Date	CVSS	vulne unaut with in multiple composed service Java S Embervulne S Embervu	rability and henticate ple protocomise Janded Schorized a partial se (partial	allows acted attact access of the color of t	cker via Java sful alt in so of of sto nning Start oxed EE 8), code the rity. also APIs ugh a PIs. J.7 . J./PR: A:L).	Pate	ch	NCIIF	PCID
N/A	16-10-2019	4.3	SE pro	erability in the control of the cont	Oracle J nt: 2D). rsions th	ava	https:// ty.netap /advisor p-20191	p.com ry/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	ch	NCIIF	PC ID
			11.0.4	and 13	Difficul	t to	0001/			
			explo	it vulner	ability					
			allow	s unauth	enticate	ed				
			attacŀ	er with	networl	K				
			acces	s via mul	ltiple					
			proto	cols to c	ompron	nise				
			Java S	E. Succe	ssful att	acks				
			of this	s vulnera	ability ca	an				
			result	in unau	thorized	d				
			ability	y to caus	e a part	ial				
				l of servi	~~					
			DOS) of Java SE. Note: This vulnerability applies to							
			vulne	rability a	applies t	0				
			Java d	leploym	ents,					
				ılly in cli						
				oxed Jav						
				cations o						
			-	pplets (i	•	E 8),				
				oad and						
				sted cod		ode				
				omes fro						
			net) and	-						
			andbox		-					
			ulnerab	-						
			-	ploited b		APIs				
				specifie						
			_	onent, e	_	ugh a				
				ervice w						
				ies data						
				3.0 Base						
			`	lability ii	mpacts)					
				Vector:	NI / A G II	I (DD				
				5:3.0/AV						
			N/UI:	N/S:U/C	.:N/I:N/	A:L).				
			CVE ID : CVE-2019-2987							
			Vulnerability in the Java				https://	securi		·
			SE, Java SE Embedded			SE, Java SE Embedded ty netann com				
N/A	16-10-2019	4.3	product of Oracle Java SE			/advisor	_	A-NET-		
,			(component: 2D).			p-20191		041119	/457	
			Supported versions that			0001/				
			are af	fected a	re Java S	E:	,			
CV Scoring Sca	ole 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				2/1						

7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS '3.0/AV:N/AC:H/PR: N/U:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988	SS	Publish Date	Publish Date CVSS Desc	ription & CVE ID		Patc	h	NCIIP	CID
8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			7u231, 8	Bu221, 11.0.4 an	nd				
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			13; Java	SE Embedded:					
unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			8u221. I	ifficult to explo	oit				
with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			vulneral	oility allows					
multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			unauthe	nticated attacke	er				
compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			with net	work access via	ı				
SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			multiple	protocols to					
attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			compro	nise Java SE, Jav	va				
vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			SE Embe	edded. Successfu	ul				
unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			attacks o	of this					
cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			vulneral	oility can result	in				
service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			unautho	rized ability to					
Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			cause a j	oartial denial of					
Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			service (partial DOS) of					
vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			Java SE,	Java SE					
Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			Embedd	ed. Note: This					
typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			vulneral	oility applies to					
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			Java dep	loyments,					
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			typically	in clients runni	ing				
applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988					_				
that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			applicat	ons or sandbox	ed				
untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988									
that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			that load	l and run					
internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			untruste	d code (e.g., cod	de				
Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			that com	es from the					
This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			internet	and rely on the	e				
This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988			Java san	dbox for securit	ty.				
apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988					-				
typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2988									
load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988									
code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988									
by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988 Vulnerability in the Oracle https://securi									
3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988 Vulnerability in the Oracle https://securi									
(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2988 Vulnerability in the Oracle https://securi				-	. 55				
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2988 Vulnerability in the Oracle https://securi									
(CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2988									
N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2988 Vulnerability in the Oracle https://securi									
CVE ID : CVE-2019-2988 Vulnerability in the Oracle https://securi			•	` ' '					
Vulnerability in the Oracle https://securi									
NI/A 14C 10 2010 A 2 VUINELADINIVIII UIE UTACIE HILLDS://SECUTI		_	Vulnara			https://s	rocuri		
N/A 16-10-2019 4.3 Vuller ability in the Oracle inteps://securi ty.netapp.com A-NET-		16-10-2019	10-10-2019 4.3	<u> </u>				A-NET-I	E-SE-
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9		cale 0-1	Scale 0-1 1-2 2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
WCarriess'			Edition Graal Java). Version 19.2.0 Vulne unaut with a multiple Graal Edition Signification addition access Oracle Edition CVSS (Integral Vector (CVSS N/UI:	on production The support that is a chenticate network ple protocomise (Communication) attack icantly in accession or most to critical procession or most t	act of Orapponent opported is affected attacked attacked attacked attacked access where the distinct of the can result or action of the can result or action of the can result of the can result of the can result or action of the can result of the	cle chis clt in on or all cprise a. b.8 VSS	/advisor p-20191 0001/	y/nta	041119	
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker				https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-NET- 041119	
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	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
			multiple compose service attack vulne unaut cause service Java Service	network ple proto romise Ja nbedded as of this rability of thorized a partia E, Java S edded. No rability a deployme ally in cli boxed Jav cations o applets (i oad and i asted cod and so and ron cally in ser and run o (e.g., cod adminis ase Score lability in Vector: S:3.0/AV N/S:U/O D: CVE-	can resurability to a deployment of the contract of the contra	ava sful It in o of of of start oxed E 8), sode the rity. es not nents, at sted ed CVSS				
N/A	16-10-2019	4	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u221;			SE at is	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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
			Java SE Embedded: 8u221.		
			Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks require human		
			interaction from a person		
			other than the attacker.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Java SE, Java SE		
			Embedded accessible data		
			as well as unauthorized		
			read access to a subset of		
			Java SE, Java SE Embedded		
			accessible data. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability does not		
			apply to Java deployments,		
			typically in servers, that		
			load and run only trusted		
			code (e.g., code installed		
			by an administrator). CVSS		
			3.0 Base Score 4.2		
			(Confidentiality and		
			Integrity impacts). CVSS		
			integrity inipacts). Cv33		

products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code	Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code				(CVSS N/UI:	S:3.0/AV R/S:U/C	::L/I:L/A	A:N).				
	N/A	16-10-2019	4	SE pr SE (co Suppo are af 7u23 13. Di vulne unaut with i multi comp Succe huma perso attack vulne attack impac produ attack vulne unaut insert some data a unaut to a si acces vulne Java o typica sandk applic Java a that le	oduct of omponer orted verificated and ifficult to be a common of the result of the re	Oracle Javadorsions the Java St., 11.0.4 of exploit allows ted attact access to ava SE. access for a construction and cessful accessful accessful accessful accessful accessful accessful access series access serie	ava loc). hat SE: and cker via quire om a e a SE, htly llt in s to sible cess This to nning Start oxed SE 8),	ty.netapy /advisor p-20191	p.com ry/nta		
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CV Scoring Sca	ale 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	Description & CVE ID				h	NCIIP	CID
			interral Java so This vapply typical load a code by an 3.0 Ba (Confintegral Vector (CVSS N/UI:	comes fromes fromes and sandbox vulnerable to Java ally in seand run (e.g., coo administase Scorrity imports its i	rely on for secupility does deployed the constant of the const	rity. es not nents, nat sted led CVSS /SS //SS //SS //SS				
N/A	16-10-2019	4.3	Vulnes SE, Jar produ (comp Suppor are af 7u23 13; Jar 8u22 vulnes unaut with multipus SE En attack vulnes unaut deleti acces Java Sacces vulnes Java Sacces vulnes Java Sacces Java Sacces vulnes vu	erability va SE En uct of Or ponent: orted ve fected a 1, 8u221 va SE En 1. Difficu rability thentica network ple prot romise onbedded so of this crability thorized son or m s to criti SE, Java S sible dat crability deploym ally in cl	in the Janbedded acle Java SLibrarie rsions the regard of the lattace access to cools to lava SE, can resurd cal data SE Embera. Note: applies the ents,	tva d a SE s). hat SE: and d: cloit cker via Java sful dit in n, ion or all edded This to	https://sty.netapy/advisorp-201910001/	p.com ry/nta	A-NET-1 041119	
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
				applied Java at that let untrue that continued in the Company web so supplied CVSS (Integrated CVSS (Integrated CVSS N/UI:	S:3.0/AV N/S:U/0	or sandb in Java S run de (e.g., com the rely on for secu- oility can object e.g., through to the A e Score 5 bacts). Com C:N/AC:H	oxed SE 8), code the rity. also APIs ugh a PIs. 5.9 VSS				
N/A	16-1	.0-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with the multi comp SE En attack vulne unaut	vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of				securi p.com ry/nta .017-	A-NET-1 041119	
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	D	escription	a & CVE II	D	Pato	:h	NCIIF	PC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2962							
N/A	16-10-2019	4.3	SE, Jar produ (comp Concu versionare Ja 11.0.4 Embe Diffica vulne unaut with a multi comp					securi p.com ry/nta 017-	A-NET- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			unaut cause service Java S Embe vulne explo data t specif withou Java V applie Java a throu CVSS (Avai CVSS (CVSS N/UI:	rability of thorized a partial a par	ability to l denial al DOS) SE ote: This can only supplying the aponent of Untrust to Service Score 3 mpacts) :N/AC:HC:N/I:N/	ted sted e. A/PR: (A:L).				
N/A	16-10-2019	4.3	Vulne SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En attack vulne unaut cause	rability va SE Emact of Oraponent: Jorted verificated and SE Emachenticated and SE Emachenticated a partial ce (partial ce (pa	in the Janbedded acle Java Start 1.0.4 abedded attacked attacked access vacces for ava SE, jacked ability the light denial	lva l a SE nat SE: and d: cloit cker via Java sful dt in co of	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	_
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
			Embervulne Java de typical sandha applied Java a that le untrue that continue in the Complex Supple CVSS (Avail CVSS (CVSS N/UI:	E, Java S dded. No rability a leployme ally in cli boxed Jav cations o applets (i boad and sted cod omes fro net) and andbox vulnerab ploited b especifie bonent, e service w ies data 3.0 Base lability in Vector: 5:3.0/AV N/S:U/C D: CVE-	ote: This applies to ents, dents run le (e.g., com the rely on the rely on the degree of the A score 3 mpacts) :N/AC:H	nning Start oxed E 8), code the rity. also APIs ugh a PIs. 5.7				
N/A	16-10-2019	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this				https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-NET- 041119	
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
			vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L). CVE ID: CVE-2019-2975		
active_iq_uni	fied_manager		0.2.2.1.0.2.2.3.2.3.2		
N/A	16-10-2019	5.8	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-ACTI- 041119/467
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	D	escription	a & CVE I	D	Pato	h	NCIIP	C ID
			explo	it vulner	ability					
			allow	s unauth	enticate	ed				
			attacl	ker with	networl	K				
			acces	s via mu	ltiple					
			proto	cols to c	ompron	nise				
			Java S	E. Succe	ssful att	acks				
			of thi	s vulnera	ability ca	an				
			result	in unau	thorized	d				
			read a	access to	a subse	et of				
			Java S	SE access	ible dat	a				
			and u	nauthor	ized abi	lity				
			to cau	ise a par	tial deni	ial of				
			servi	ce (partia	al DOS)	of				
			Java S	E. Note:	This					
			vulne	rability a	applies t	to				
			· ·	leploym						
				ally in cli						
				oxed Jav						
			appli	cations o	r sandb	oxed				
			-	ipplets (i	-	E 8),				
				oad and						
				sted cod		ode				
				omes fro		_				
				net) and	-					
				andbox		-				
				ulnerab/	,					
				to Java						
				ally in se						
				and run o						
				(e.g., cod						
			-	adminis	,	CVSS				
				ase Score						
			-	identiali	_					
				ability in	ipacts).	CVSS				
			Vecto							
			`	5:3.0/AV	•	•				
			N/UI:	N/S:U/C	::L/I:N/	A:L).				
			CVE ID : CVE-2019-2977							
			Vulnerability in the Java				https://s	securi	A-NET-	Δ <i>С</i> ТΙ₋
N/A	16-10-2019	4.3	SE, Java SE Embedded				ty.netapp.com		041119	
				ict of Ora			/advisor	-	041119	7 700
CV Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1		2 3	252	+ 3	30		, 0	0 9	3 10

Weakness	Publish Date	cvss	Description	n & CVE II	D	Pato	h	NCIIP	CID
			(component:	Networl	king).	p-20191	017-		
			Supported ve	ersions th	nat	0001/			
			are affected a	ire Java S	E:				
			7u231, 8u22	1, 11.0.4	and				
			13; Java SE E	mbedded	l:				
			8u221. Diffic	ult to exp	oloit				
			vulnerability	allows					
			unauthentica		ker				
			with networl	c access v	⁄ia				
			multiple prot	cocols to					
			compromise		ava				
			SE Embedded	-					
			attacks of thi						
			vulnerability		lt in				
			unauthorized						
			cause a partia						
			service (part						
			Java SE, Java	-					
			Embedded. N		,				
			vulnerability						
					.0				
			Java deploym		nina				
			typically in cl		_				
			sandboxed Ja						
			applications						
			Java applets (•	E8J,				
			that load and		,				
			untrusted co		ode				
			that comes fr						
			internet) and	-					
			Java sandbox		-				
			This vulneral	-					
			be exploited	by using	APIs				
			in the specifi	ed					
			Component,	e.g., thro	ıgh a				
			web service v	which					
			supplies data	to the A	PIs.				
			CVSS 3.0 Base	e Score 3	.7				
			(Availability	impacts)	.				
			CVSS Vector:						
			(CVSS:3.0/AV	/:N/AC:H	I/PR:				
			N/UI:N/S:U/	•	′				
	<u> </u>								
CV Scoring Sca	ole 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-1

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2978		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-NET-ACTI-041119/469
CV Scoring Sca	ale 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	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	CID
				CVSS (CVSS N/UI:	lability i Vector: 5:3.0/AV N/S:U/0 D : CVE -	:N/AC:H C:N/I:N/	I/PR: A:L).				
NSA				CVEI	D. CVE	2017-2	773				
ghidra											
Untrusted Search Path	16-	10-2019	4.4	uses a untru When from proce is set when Pytho "Ghid Wind Ghidr the cr this w	Ghidra the potential sted sea a given personal sea work to this personal launching a Code ow > Pyra will trandexe personal sea will be	rch path ng Ghid path, the ing direct ath. The oreter vi- browser thon" or y to exect rogram director	n. ra e Java ctory en, a the r> otion, cute from	N/A		A-NSA-041119	
Untrusted Search Path	16-	10-2019	4.4	NSA Ghidra before 9.0.2 is vulnerable to DLL hijacking because it loads jansi.dll from the current working directory. CVE ID: CVE-2019-17665		N/A		A-NSA- 041119			
Openafs											
openafs											
Deserializati on of Untrusted Data	29-	10-2019	5	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to denial of service from unserialized data access because remote attackers can make a							
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pato	h	NCIIP	CID
			calls t serve SVOT handl	D : CVE-	a databa the g RPC					
Information Exposure	29-10-2019	5	and 1 prone disclo becau scalar netwo	AFS before to an income to an income with the second of th	re 1.8.5 Iformati Inerabili tialized nt over t peer.	is on ty	N/A		A-OPE-0 041119	
Information Exposure	29-10-2019	4.3	and 1 prone leakaş condi unini varial netwo	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to information leakage upon certain error conditions because uninitialized RPC output variables are sent over the network to a peer.		N/A		A-OPE-0 041119		
				CVE ID : CVE-2019- 18603						
Open-emr										
openemr										
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	21-10-2019	6.5	Authenticated SQL Injection in interface/forms/eye_mag/ js/eye_base.php in OpenEMR through 5.0.2 allows a user to extract arbitrary data from the openemr database via a non-parameterized INSERT INTO statement, as demonstrated by the			N/A		A-OPE-0 041119		
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
			providerID parameter. CVE ID : CVE-2019- 16404		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	Reflected XSS in interface/forms/eye_mag/ view.php in OpenEMR 5.x before 5.0.2.1 allows a remote attacker to execute arbitrary code in the context of a user's session via the pid parameter. CVE ID: CVE-2019-16862	N/A	A-OPE-OPEN- 041119/476
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	Reflected XSS exists in interface/forms/eye_mag/view.php in OpenEMR 5.x before 5.0.2.1 ia the id parameter. CVE ID: CVE-2019-17409	N/A	A-OPE-OPEN- 041119/477
openwrt					
openwrt					
Cross-Site Request Forgery (CSRF)	https://githu b.com/openw rt/luci/comm it/f8c6eb67cd 9da09ee2024 8fec6ab74206 9635e47	A-OPE-OPEN- 041119/478			
Oracle					
CV Scoring Sca (CVSS)	ole 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escription	ı & CVE II	D	Pato	h	NCIIP	CID
retail_custon	ner_managemo	ent_and	d_segn	nentatio	n_found	dation				
Incorrect Authorizatio n	16-10-2019	4.9	Retail Mana Segm produced Appli Segm version 17.0. Vulne privil network to con Retail Mana Segm Succession and Segm Succession and Segm Custo	erability I Custom gement a entation act of Ora cations (ent). The on that is Easily ex erability a eged atta ork acces mpromis I Custom gement a entation essful atta in interac on other a exer. Succ ex of this erability of thorized tor delet of Oracl omer Man egmenta dation ac as well as thorized tor delet of Oracl omer Man egmenta dation ac essor acces cas of this erability of thorized tor delet of Oracl omer Man egmenta dation ac essor acces cas of this erability of thorized tor delet of Oracl on other egmenta dation ac essor acces cas of this erability of thorized thorized thorized thorized thorized acces cas of this erability of thorized thorized thorized thorized thorized thorized acces cas of this erability of thorized	er and Foundar acle Retar comports affected apploitable allows le acker with a Foundar acks requestion from the essful can resurupdate, accessible agemention agemention agemention agemention accessible agemention accessible accessi	ation ail nent: rted d is le ow ith TTP e ation. quire om a e cess Retail nt e core nd SS	N/A		A-0RA- 041119	
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	D	escriptio	n & CVE II	D	Pato	:h	NCIIP	C ID
			CVE I	D : CVE-	2019-2	883				
Information Exposure	16-10-2019	4.3	Retail Mana Segm produced Appli Segm version 17.0. vulne unaut with a HTTP Oracle Mana Segm Succes vulne unaut critical access Custo and S Found data. 5.9 (Cimpad (CVSS N/UI:	rability Custom gement entation act of Or cations (ent). The on that is Difficult rability a chenticat network to comp e Retail (gement entation ssful att rability chorized al data o s to all O mer Man egment dation ac CVSS 3.0 Confiden cts). CVS S:3.0/AV N/S:U/O D: CVE-	rer and Foundate Retares supports affected to explorate access where the complete access to explorate acce	ation ail nent: rted d is oit cker ria er ation. chis alt in co ete etail nt core :: I/PR: A:N).	N/A		A-ORA-1 041119	
mysql										
N/A	16-10-2019	4.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Difficult			https:// ty.netap /advisor p-20191 0002/	p.com y/nta	A-ORA- 041119	•	
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
			to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2910		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/482

Weakness	Publish	Date	cvss	D	Description & CVE ID			Pate	ch	NCIIF	PC ID
				H/UI:	N/S:U/	C:L/I:N/	A:N).				
				CVE I	D : CVE	2019-2	911				
N/A	16-10-2	2019	4	Serve MySQ Serve Encry versic are 5. 8.0.1.2 explo allow attack proto MySQ attack vulne unaut cause repea (comp Serve Score impac (CVSS L/UI:	or production producti	ity: Support are affect d prior a ior. Easi ulnerabi ivileged networ ltiple compron r. Succes can resu ability t or frequ ash S) of My 3.0 Base ailability S Vector (:N/AC:L	ed cted nd ly lity k nise ssful alt in co ently rSQL r: -/PR: -/PR: -/A:H).	https://ty.netap/advisorp-20191	p.com ry/nta	A-ORA- 041119	•
Incorrect Authorizatio n	16-10-2	2019	5	CVE ID: CVE-2019-2914 Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). Supported versions that are affected are 5.3.13 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via				N/A		A-ORA- 041119	•
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

Information Exposure Information Exposure	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Underability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N).				compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:N/I:N/A:L).		
		16-10-2019	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N).	ty.netapp.com /advisory/nta p-20191017-	_

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
Information Exposure	16-10-2019	5	Serve MySQ Serve Encry version are 5. 5.7.27 exploi allow attack acces proto MySQ attack vulne unaut to a si Serve CVSS (Confi CVSS (CVSS N/UI:	, ,	ct of Oraconent: cty: Supported are affect l prior a cor. Easilular abilular abilula	cle ed cted nd ly lity ed ssful lt in cess a3 cts). /PR: A:N).	https://ty.netap/advisorp-20191	p.com ry/nta	A-ORA- 041119	•
Information Exposure	16-10-2019	5	Serve MySQ Serve Encry versionare 5. 5.7.27 exploi allow attack acces proto MySQ	N/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2923 Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this				securi p.com ry/nta .017-	A-ORA- 041119	•
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	Pu	blish Date	e CVSS		escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				to a s Serve CVSS (Conf CVSS (CVSS N/UI	thorized ubset of er access 3.0 Base fidential Vector: S:3.0/AV :N/S:U/O	MySQL ible data e Score 5 ity impa V:N/AC:L	a. 5.3 cts). /PR: A:N).				
Improper Input Validation	16-	10-2019	3.5	Serve MySC Innol versicare 5 8.0.1 to expand attack access proto attack unau cause (com Serve Score impa (CVS) H/UI	erability er produ ()L (comp ()DB). Sup ()OB). Sup ()OB	ct of Oraconent: ported are affect d prior a ior. Diffi nerabilit rivileged network litiple compron r. Succes can resu ability t or frequ ash OS) of My 3.0 Base ailability S Vector V:N/AC:H C:N/I:N/	cted nd cult cy d k nise sful dt in co ently cSQL c: H/PR:	https://s ty.netap /advisor p-20191 0002/	p.com ry/nta	A-ORA- 041119	-
N/A	16-	10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.27 and prior and				https://s ty.netap /advisor p-20191 0002/	p.com ry/nta	A-ORA- 041119	•
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:U/C:N/I:N/A:H).							
			CVE I	D : CVE-	2019-2	946				
N/A	16-10-2019	4	Serve MySQ Serve Suppo are af prior Easily vulne privil netwo multi- comp Serve of this result ability frequ- crash MySQ Base S	rability reproduce L (comported version of the comported and 8.0.) resploits reproduced and 8.0. resploits reproduced accessive ple protocomise Mark accessive vulneration unauty to caussently reproduced to the complete L Server Score 4.5 lability in lability	et of Oraconent: izer). rsions the sions the sions the allows he acker with sions to MySQL asful attached a hange et a hange et e DOS) r. CVSS 3	cle nat 6 and orior. igh ith acks an d g or of 8.0	https:// ty.netap /advisor p-20191 0002/	p.com ry/nta	A-ORA- 041119	•
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
N/A	16-10-2019	4	CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2948 Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2982	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/491
N/A	16-10-2019	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.017 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/492
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			Serve of this result ability frequences to the serve of this result ability frequences of the serve of the se	romise Nor. Successor vulneration unauty to cause ently republication of MySQ sible date Score 5.5 vailability Vector: Si.3.0/AV N/S:U/Q	ability can thorized thorized to a hang peatable ete DOS) as well update, te access L Serve a. CVSS (Integraty impacts)	an d g or of as s to r 3.0 rity cts).				
			CVE I	D : CVE-	2019-2	991				
N/A	16-10-2019	3.5	Serve MySQ Serve versic are 5. 8.0.17 to exp allow attack proto MySQ attack vulne unaut cause repea (comp Serve Score impac	rability r produce L (compose that a compose that a compose to compose the compose table crability of table	ct of Oraconent: . Supportance affects are affects l prior a or. Difficience bilitiation of the compronents can resurb ash S) of My 3.0 Base biliability S Vector	cle rted cted nd cult cy k nise sful dt in co ently rSQL	https://ity.netap /advisor p-20191 0002/	p.com ry/nta	A-ORA- 041119	•
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
			L/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2993		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: H/UI:N/S:U/C:N/I:N/A:H).	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/494
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/495
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pu	blish Date	e CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
				ability frequence crash MySQ Base (Avaite CVSS (CVSS H/UI)	t in unauty to cause ently rejection (complete) Score 4.9 lability in Vector: 5:3.0/AV	se a hang peatable ete DOS) r. CVSS 3 9 mpacts) ':N/AC:L C:N/I:N/	g or () of 3.0 (. ./PR: (A:H).				
N/A	16-	10-2019	4	Serve MySQ InnoI versic are 8 explo allow attack proto MySQ attack vulne unau cause repea (com Serve Score impa (CVSS H/UI	erability or product of (composite points). Suppose that of (0.16) and itable voints high points of the collection of this erability thorized of the collection of the collection of this erability thorized of the collection of the collection of this erability thorized of the collection of the collect	ct of Oraconent: ported are affect are affect diprior. Indinerability to comproner. Success can resurability to ash S) of My 3.0 Base ailability S Vector S':N/AC:L C:N/I:N/	cted Easily lity d k hise ssful alt in co ently rSQL r: L/PR:	https://ty.netar/advisop-20190002/	p.com ry/nta	A-ORA- 041119	•
N/A	16-	10-2019	4	Serve MySQ Serve	erability or produce OL (comp or: Parse ons that	ct of Ora oonent: r). Supp	orted	https:// ty.netar /adviso p-2019 0002/	p.com ry/nta	A-ORA- 041119	-
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			explo allow attack acces proto MySQ attack vulne unaut cause repea (comp Serve Score impac (CVSS	0.17 and itable vus s low pricer with s via muscols to coll Server as of this rability of thorized a hang of table craplete DO r. CVSS 3 6.5 (Avacts). CVS	Ilnerabilivileged networl ltiple ompron Succes can resu ability t or freque ash S) of My 3.0 Base ailability S Vector	lity k nise sful dit in co ently rSQL r ::				
			CVE I	D : CVE-	2019-3	004				
N/A	16-10-2019	4	Serve MySQ Serve Suppo are af prior. vulne privil netwo multi comp Serve of this result ability frequ crash MySQ Base (Avail	erability or produce of (composite for the composite of t	et of Ora conent: ection). rsions the re 8.0.17 to expl allows he acker with acker with ss via ocols to MySQL ability cat thorized thorized e a hang beatable ete DOS)	cle nat 7 and oit igh ith acks an d g or of 3.0	https:// ty.netap /advisor p-20191 0002/	p.com y/nta	A-ORA- 041119	•
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
			(CVSS:3.0/AV:N/AC:H/PR: H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-3009		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-3011	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/499
Improper Input Validation	16-10-2019	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/500
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	Pul	blish Date	e C	CVSS	Description & CVE ID				Pato	:h	NCIIP	C ID
					result ability frequ crash MySQ Base (Avai CVSS (CVSS H/UI:	s vulner to the tin unauty to cause ently report (complete) L Server 1 (complete) L Server 1 (complete) Se	ethorized se a hang peatable ete DOS) c. CVSS 3 4 mpacts) :N/AC:H	d g or of 3.0 I/PR: (A:H).				
N/A	16-	10-2019	4	1	Serve MySQ Serve Suppo are af prior vulne privil netwo multi comp Serve of thi result ability frequ crash MySQ Base (Avai CVSS (CVSS H/UI:	erability or product of comported ve ffected a fected a fected att ork acce ple prote or Succes s vulner t in unau y to caus ently rep (comple of Score 4.6 lability i Vector: 6:3.0/AV	ct of Oraconent: nizer). rsions the second with acker we so via acker we so via ability cathorized a hange actable act	nat 6 and 6 and 6 and 6 and 6 igh ith acks an d g or 6 of 8.0	https://ty.netap/advisorp-20191	p.com ry/nta	A-0RA- 041119	•
N/A	16-	10-2019	9 4	1	Vulnerability in the MySQL Server product of Oracle MySQL (component:			https:// ty.netap /advisor	p.com	A-ORA- 041119		
CV Scoring Sca (CVSS)	ale	0-1	1-2	2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	1 & CVE I	D	Pato	:h	NCIIF	PC ID
			Encry versic are 8. explo allow attack proto MySQ attack vulne unaut cause repea (comp Serve Score impac (CVSS H/UI:	r: Securion). Sons that a constant of the constant of this rability of the constant of the con	Supported are affect are affect are affect affect affect are affect are affect	cted Easily lity l k hise sful lt in co ently rSQL r: ./PR: ./PR:	p-20191 0002/	017-		
N/A	16-10-2019	4	Serve MySQ Serve Suppo are af prior Easily vulne privil netwo multi comp Serve of this result ability frequ	rability r produce L (comp r: Replice rected and 8.0. rexploita rability a eged atta ork acces ple proto romise M r. Succes s vulnera in unau y to caus ently rep (comple	et of Oraconent: cation). rsions the sions the sions the callows he cacker with six via cools to MySQL asful attacherized thorized to eatable coestable.	nat 7 and prior. ligh ith	https:// ty.netap /advisor p-20191 0002/	p.com y/nta	A-ORA- 041119	_
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	Pub	lish Date	CVSS	Description & CVE ID				Pato	h	NCIIP	CID
Weakness N/A		lish Date	4	MySQ Base (Avai CVSS (CVSS H/UI: CVE I Vulne Serve MySQ InnoI versic are 8. explo allow attacl acces proto MySQ attacl vulne unaut cause repea (com; Serve	(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2960 Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base			https://s ty.netapj /advisor p-20191 0002/	securi p.com	A-ORA- 041119	MYSQ-
				impa (CVSS H/UI:	4.9 (Ava cts). CVS 5:3.0/AV N/S:U/C D : CVE	S Vector :N/AC:L C:N/I:N/	r: ./PR: 'A:H).				
N/A	16-1	.0-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with				https://s ty.netapp /advisor p-20191 0002/	p.com ry/nta	A-ORA- 041119	-
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
			network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:U/C:N/I:N/A:H).		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:U/C:N/I:N/A:H).	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/506

4-5

5-6

6-7

7-8

8-9

9-10

1-2

0-1

2-3

CV Scoring Scale

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2967		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: H/UI:N/S:U/C:N/I:N/A:H).	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/507
			CVE ID : CVE-2019-2968		
Information Exposure	16-10-2019	2.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks	https://securi ty.netapp.com /advisory/nta p-20191017- 0002/	A-ORA-MYSQ- 041119/508

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Pub	lish Date	e CVS	S	D	escriptio	1 & CVE I	D		Patc	h	NCIIP	C ID
				read coordinates of the coordina	esult cces omp lySQ ata. .2 (C npac CVSS /UI:	s vulner; t in unau s to criti lete acce L Server CVSS 3.0 Confiden cts). CVS S:3.0/AV N/S:U/C D: CVE-	thorized cal data ess to all accessi Base So tiality S Vector :L/AC:L C:H/I:N/	d or ble core r: /PR: (A:N).					
N/A	16-1	.0-2019	4	Se M Se Si ar pri 8. ex al at ac pri M at vi ur ca se Si im (C L,	erve lySQ erve uppo ce af rior, 0.17 0.17 explo llow ttack ttack ttack ulne ause epea comp erve core mpao CVSS /UI:	erability or produce of (comported verificated are of 5.7.27 are of and privilent of the color to colo	ct of Oraconent: lizer). rsions the second prior for. Easily linerability leged metwork can resurability to frequency ash S) of My 3.0 Base hilability S Vector :N/AC:L	nat 5 and r and ly lity k nise ssful alt in co ently rSQL r: -/PR: -/PR: -/A:H).	ty /a p-	ttps://s v.netapj advisor -20191 002/	o.com y/nta	A-ORA- 041119	•
jdk													
N/A	16-1	.0-2019	4.3	•				ttps://s ⁷ .netapj		A-ORA-	JDK-		
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-	-3	3-4	4-5	5-6		6-7	7-8	8-9	9-10

product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AN:N/AC:H/PR: N/U!:N/S:U/C:L/I:N/A:N).	Weakness	Publish Date	CVSS	Descri	ption & CVE	ID	Pato	h	NCIIP	CID
Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				product o	f Oracle Jav	ra SE	/advisor	y/nta	041119	/510
are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				(compone	ent: Securit	y).	p-20191	017-		
7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				Supported	d versions	that	0001/			
13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				are affect	ed are Java	SE:				
8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				7u231, 8u	ı221, 11.0.	4 and				
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS'3.0/AV:N/AC:H/PR:				13; Java S	E Embedd	ed:				
unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				8u221. Di	fficult to ex	xploit				
with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				vulnerabi	lity allows					
multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS'3.0/AV:N/AC:H/PR:				unauthen	ticated atta	acker				
compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS'3.0/AV:N/AC:H/PR:				with netw	ork access	via				
compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS'3.0/AV:N/AC:H/PR:				multiple p	orotocols to)				
SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				_	-	-				
vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				attacks of	this					
unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS'3.0/AV:N/AC:H/PR:						ult in				
to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					-					
SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					•					
vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						, ibic				
Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						: to				
typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					=	ınning				
applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						_				
Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					•	SE OJ,				
that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				0110101010						
internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						code				
Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						.1				
This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				_	-					
be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						-				
in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						g APIs				
web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				_						
supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				_	_	ough a				
CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
(Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				CVSS 3.0 1	Base Score	3.7				
(CVSS:3.0/AV:N/AC:H/PR:				(Confiden	itiality imp	acts).				
				CVSS Vect	tor:					
N/UI:N/S:U/C:L/I:N/A:N).				`		•				
				N/UI:N/S	:U/C:L/I:N	/A:N).				
CV Scoring Scale										

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2894		
Information Exposure	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-ORA-JDK- 041119/511
CV Scoring Sca					

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			CVSS (Conf CVSS (CVSS N/UI:	ies data 3.0 Base identiali Vector: 3:3.0/AV R/S:U/C D:CVE -	Score 3 ty impac :N/AC:H :L/I:N/A 2019-2	.1 cts). I/PR: A:N). 933				
N/A	16-10-2019	2.6	SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with a multipor se En attack interaction other Succes vulne unaut cause service Java Se Ember vulne Java de typica sandk applied Java attack interaction of the service service java Se Ember vulne Java de typica sandk applied java attack interaction of the service java Se Ember vulne Java de typica sandk applied java attack interaction of the service service java Se Ember vulne java de typica sandk applied java attack interaction of the service service java	va SE Emoret of Oraconent: It of Oraconent: It or of Oraconent: It or of Oraconent: It	nbedded acle Java Network rsions the sions the sions the sions the sions access where access we cools to ava SE, J. Success the human aper exactacked actacks of the can result ability the sions access the sions applies the can result ability the sions access where side access of the can result ability the can result ability the sions access the can result ability the sions access the can result ability the can result ability the sions access the can result ability the can result ability the sions access the can result ability the can result abil	s SE king). at SE king). at SE: and d: claim of ser. at sful in son er. chis lt in sof of ser. cava start oxed E 8),	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA-) 041119	
CV Scoring Sca	le 0-1	1-2	2-3			5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pato	:h	NCIIP	C ID
			Java s This v apply typica load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	net) and andbox fulnerabet of Java of ally in second administrates as Score lability in Vector: S:3.0/AV R/S:U/C D: CVE-	for secuility doe deploymers, the only trusted install trator). A second control of the control	rity. es not nents, nat sted ed CVSS . I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Support are aff 7u23; Ja 8u22; vulne unaut with a Kerber Java S Ember vulne Java S addition Successive unaut critical accessive SE Endata.	erability in the property of t	nbedded acle Java Kerbero rsions the re Java S , 11.0.4 nbedded alt to exp allows red attace access v omprom E hile the access v other java dded, attace acks of t can resu access t r comple accessil accessil is	s). at sE; and d: cleicand dise asE, tacks act this lt in o ete ava ble	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6							

Weakness	Publish Date	cvss	D	escription	ı & CVE II	D	Pato	:h	NCIIP	PC ID
			typical sandbapplical sandbapp	leploymedally in clipoxed Jave cations of applets (in oad and standbox from the candbox fro	ents rur va Web S r sandb in Java S run ie (e.g., c om the rely on t for secu ility can by using d ig., throu which to the A Score 6 ty impact :N/AC:H :H/I:N/	Start oxed oxed EE 8), code the rity. also APIs ugh a PIs. 8 cts).				
N/A	16-10-2019	5.8	SE prosection SE prosection SE (consumption SE	erability in oduct of componer or ted vere fected and 13. It wilners with the cols to constant of the cols to constant or the cols and the cols to constant or the cols to constant or the cols to constant or the cols and the cols and the cols are constant or the cols and the cols are constant or the cols and the cols are constant or	Oracle Jat: Hotspersions the Java Son Difficult ability denticated ompromessful attractions a subsectible data dentical	ava pot). nat EE: t to ed cacks an d et of a lity ial of	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	-
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	PC ID
			vulne Java d typica sandh applica Java a that le untru that c interr Java s This v apply typica load a code o by an 3.0 Ba (Conf Availa Vecto (CVSS N/UI:	E. Note: rability a leploymonally in clipoxed Java cations of polets (in oad and exted code and box and box and run of le.g., code administication administication of the cation of the cation of the cation of le.g., code administication of le.g., code administration of le.g., code	applies tents, lents run le (e.g., com the rely on the rely on the rely only trus le install strator). Le 4.8 ty and apacts).	nning Start oxed SE 8), code the rity. es not nents, nat sted led CVSS L/PR: A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with n multi- comp SE En	erability va SE En act of Ora ponent: I orted ver fected ar 1, 8u221 va SE En 1. Difficu rability a thenticat network ple proto romise J nbedded	nbedded acle Java Network rsions the re Java S , 11.0.4 nbedded alt to exp allows ted attact access to access to ava SE, J	d SE king). nat SE: and d: oloit cker via	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	-
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			unaut cause service Java S Embe vulne Java d typica sandh applie Java a that le untru that c interregion Java s This very be expired to the Compe web service (CVSS (CVSS N/UI:	rability of thorized a partial a partial are (partial are (partial are (partial are	ability to l denial al DOS) of SE ote: This applies to ents, dents run le (e.g., com the rely on the rely on the lility can by using downlich to the A secore 3 mpacts) :N/AC:H	of of of of sto oning Start oxed SE 8), code the rity. also APIs ugh a PIs. 5.7 .				
N/A	16-10-2019	4.3	SE, Japrodu (composupped are af 7u23: 13; Ja 8u22: vulne unaut	erability va SE En ponent: J ported ver fected an 1, 8u221 va SE En 1. Difficu rability a chenticat network	nbedded acle Java JAXP). rsions the re Java S ., 11.0.4 nbedded alt to exp allows ted attace	l a SE nat SE: and d: oloit	https://sty.netapgi /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	
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	De	scription	a & CVE I	D	Pato	h	NCIIP	PC ID
			compress Embed vulner unauth cause a service Java SI Embed vulner Java de typical sandbe applicated	bedded sof this rability of a partial e (partial e (partial e (partial e (partial e e (p	ava SE, job and results ability to a denial al DOS) of E applies to a more and before an	sful alt in co of of sto nning Start oxed SE 8), code the rity. also APIs ugh a PIs. 3.7 . d/PR:				
N/A	16-10-2019	4.3	SE, Jav produc (comp Seriali version are Jav	a SE Emet of Oraconent: zation). ns that a	in the Janbedded acle Java Support are affect 1231, 81	ted cted u221,	https://s ty.netap /advisor p-20191 0001/	p.com y/nta	A-ORA- 041119	
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	D	escription	n & CVE I	D	Pato	h	NCIIP	CID
			Diffic vulne unaut with multi	edded: 80 ult to experability a thenticat network ple proto romise J	ploit allows ted attac access v	via				
			attacl vulne unaut cause service	nbedded cs of this rability of thorized a partia ce (partia	can resu ability t l denial al DOS)	alt in co of				
			Embe vulne Java o typica sandl	SE, Java Sedded. No rability a leploymoally in clipoxed Javantons of the sections of the secti	ote: This applies t ents, ents rui va Web	to nning Start				
			Java a that le untru that c interi	cations on applets (in post and and and comes fromes fromet) and	in Java S run le (e.g., o om the rely on	SE 8), code the				
			This was be expended in the Comp	andbox vulnerab ploited b specifie ponent, e service w	ility can y using d .g., thro	also APIs				
			suppl CVSS (Avai CVSS (CVSS N/UI:	ies data 3.0 Base lability in Vector: S:3.0/AV	to the A Score 3 mpacts) :N/AC:H ::N/I:N/	8.7 I/PR: 'A:L).				
N/A	16-10-2019	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: 2D).				https://s ty.netap	p.com	A-ORA- 041119	
CV Scoring Sca (CVSS)	o-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pato	h	NCIIF	CID
			are af 11.0.4 explo allow attack access proto Java S of this result ability denia DOS) vulne Java de typica sandhaplic Java atthat le untru that cointerr Java s This very be explined the Compared to the Compared Supplication (CVSS (Available) (CVSS (CVSS N/UI:	orted verificated and 13. it vulner is unauth as via multiple color to color to cause of Java Stability and and boxed Java Stability and and boxed and and boxed and and boxed julnerabe ploited be specificated and and and and boxed julnerabe ploited be specificated and and and and boxed julnerabe ploited be specificated and and and and and and and and and an	re Java S Difficul rability lenticate networl ltiple ompron ssful att ability ca thorized e a part ce (part E. Note: applies t ents, ents run a Web S r sandb in Java S run le (e.g., c om the rely on for secu ility can by using d leg., through to the A Score 3 mpacts) EN/AC:H EN/I:N/	EE: It to ed k hise cacks an d ial cial cial oxed EE 8), code the rity. also APIs ugh a PIs. E.7 . I/PR: I	p-20191 0001/	017-		
N/A	16-10-2019	4.3	SE, Ja produ	erability in the second	nbedded acle Java	l	https://s ty.netap /advisor p-20191	p.com ry/nta	A-ORA- 041119	
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	D	escription	1 & CVE I	D	Patc	h	NCIIP	CID
			Supp	orted ve	rsions th	nat	0001/			
			are af	fected a	re Java S	SE:				
			7u23	1, 8u221	, 11.0.4	and				
			13; Ja	va SE En	nbedded	d:				
			8u22	1. Difficu	ılt to exp	oloit				
			vulne	rability a	allows					
			unau	thenticat	ed attac	ker				
			with	network	access v	<i>r</i> ia				
			multi	ple proto	ocols to					
			comp	romise J	ava SE, J	lava				
			SE En	nbedded	. Succes	sful				
			attacl	ks of this						
			vulne	rability (can resu	lt in				
			unaut	thorized	ability t	:0				
			cause	a partia	l denial	of				
			servi	ce (partia	al DOS)	of				
			Java S	SE, Java S	SE					
			Embe	dded. No	ote: This	5				
			vulne	rability a	applies t	to				
			Java d	leploym	ents,					
			typica	ally in cli	ents rui	ning				
			sandl	oxed Jav	va Web S	Start				
			appli	cations o	r sandb	oxed				
			Java a	ipplets (i	in Java S	E 8),				
			that l	oad and	run					
			untru	sted cod	le (e.g., c	ode				
			that c	omes fro	om the					
			interi	net) and	rely on	the				
				andbox	-					
			· -	zulnerab		-				
				to Java o	-					
				ally in se						
				and run o						
				(e.g., cod	-					
				adminis						
			_	ase Score	_					
			-	(Availability impacts). CVSS Vector:						
				S:3.0/AV	:N/AC:F	I/PR:				
			-	N/S:U/C	-	-				
			,	D : CVE -	, ,					
			CVEI	D:CVE-	2019-2	700				l
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 Da	te CVSS	D	escription	ı & CVE II)	Pato	:h	NCIIP	C ID
N/A 16-10-201	9 4.3	Graal Edition Graal In Edition In	S:3.0/AV: :N/S:C/C	rprise act of Ora aponent: aported affected by affected attac access v acce	d is loit ker via cle his lt in on or all prise a8 VSS	https://sty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	•
N/A 16-10-201	9 4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit				https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	-
CV Scoring Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	D	Pate	ch	NCIIF	C ID
weakness	Publish Date	CVSS	vulne unaut with in multiple composed service Java Servic	rability and henticate ple protocomise Jandedded as of this rability of the control of the contr	allows ed attace access we access we access ava SE, J Success can resu ability t I denial al DOS) o E ote: This applies t ents, ents run e (e.g., c om the rely on t for secu ility doe deploym rvers, the only trus e install trator). e 3.7 mpacts) eN/AC:H ::N/I:N/ 2019-2 in the Ja	eker via lava sful lt in to of of late of late of late of late oxed let entry. es not let ed late of late of late oxed let ed late oxed	https://		NCIII	
N/A	16-10-2019	4	SE, Java SE Embedded product of Oracle Java SE (component: Deployment). The			https:// ty.netap /advisor p-20191	p.com ry/nta	A-ORA- 041119		
CV Scoring Scal		1-2	2-3							

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			supported version that is	0001/	
			affected is Java SE: 8u221;		
			Java SE Embedded: 8u221.		
			Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks require human		
			interaction from a person		
			other than the attacker.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Java SE, Java SE		
			Embedded accessible data		
			as well as unauthorized		
			read access to a subset of		
			Java SE, Java SE Embedded		
			accessible data. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability does not		
			apply to Java deployments,		
			typically in servers, that		
			load and run only trusted		
			code (e.g., code installed		
			by an administrator). CVSS		
			3.0 Base Score 4.2		

Weakness	Publish Date	cvss	D	escription	& CVE II	D	Pato	h	NCIIP	C ID
			Integrated Vector (CVSS N/UI:	identiali rity impa r: 5:3.0/AV R/S:U/C D : CVE- rability i	ncts). CV :N/AC:H :L/I:L/ <i>F</i> 2019-2	/PR: A:N). 996				
N/A	16-10-2019	4	SE pr SE (co Suppo are af 7u23 13. Di vulne unaut with i multi comp Succe huma perso attack vulne attack impac produ attack vulne unaut insert some data a unaut to a si acces vulne Java c typica sandk applic	oduct of omponer orted verificated and litty and litty and litty in the rability in the rability of the rabili	Oracle Jat: Javad rsions the Java St., 11.0.4 exploit allows red attactances while the sin Java gnificant cessful can resulupdate, access a read access a re	ava oc). at E: and ker via uire om a e a SE, atly lt in s to sible cess This co aning Start oxed	https://sty.netapy/advisorp-201910001/	p.com ry/nta	A-ORA-) 041119	
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	D	escription	a & CVE II	D	Pato	h	NCIIP	CID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:R/S:C/C:L/I:L/A:N).							
			CVE I	D : CVE-	2019-2	999				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with I multi comp SE En attack vulne unaut deleti acces: Java Sacces: Java Sacces:	erability in a SE Emporent: I ported verificated and I, 8u221 va SE Emporent: I ported and I, 8u221 va SE Emporent in a section of the sectio	nbedded acle Java Librarie. Isions the Java S, 11.0.4 abedded attacked attacked access vocols to ava SE, J. Succes can resure access can r	s). a SE s). at EE: and d: bloit eker via fava sful lt in n, on or all dded This	https://sty.netapgi /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	
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	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			typical sandbapplical sandbapp	S:3.0/AV N/S:U/C	ents rur va Web S r sandb in Java S run le (e.g., c om the rely on t for secu ility can by using d leg., through to the A Score 5 eacts). C' EN/AC:H	Start oxed oxed EE 8), code the rity. also APIs ugh a PIs. 5.9 VSS				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En attack vulne	N/UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2958 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to				securi p.com ry/nta 017-	A-ORA- 041119	
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	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			service Java S Ember vulne Java de typical sandh applice Java a that le untru that control interrest Java service This was a supple Competer Supple CVSS (Available CVSS (CVSS N/UI:	ce (partial E, Java S dded. No rability a leployme ally in clipoxed Javations of pplets (in sted codes and box	al DOS) of EE ote: This applies to ents, ents run are (e.g., com the rely on the for securility can by using deg., through to the A Score 3 mpacts) :N/AC:H	of sto nning Start oxed sE 8), code the rity. also APIs ugh a PIs. 5.7 . I/PR: (A:L).				
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java			https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-ORA- 041119	•	
CV Scoring Scal										

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			attack vulne unaut cause service Java S Embe vulne explo data t specif witho Java V applie Java a throu CVSS (Avail CVSS (CVSS N/UI:	nbedded as of this rability of thorized a partia as (partia as (pa	can resurability to ability to learn ability to learn an including the ponent to learn as to service a score 3 mpacts) :N/AC:H ::N/I:N/	lt in of of of s be g ted sted c7 . I/PR: A:L).				
N/A	16-10-2019	4.3	CVE ID: CVE-2019-2964 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to			https://sty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	•	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			service Java S Ember Vulne Java d typica sandh applice Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	a partia ce (partia ce (partia ce), Java S dedd. No rability a leployme ally in cli boxed Jav cations o applets (i boad and sted cod omes fro net) and andbox vulnerab ploited b especifie conent, e ervice w ies data 3.0 Base lability in Vector: 6:3.0/AV N/S:U/C D: CVE-	al DOS) SE ote: This applies a ents, lents run or sandb in Java S run le (e.g., o om the rely on for secu ility can oy using d .g., thro which to the A e Score 3 mpacts) :N/AC:H C:N/I:N/	of sto nning Start loxed SE 8), code the rity. also APIs ugh a .PIs. 8.7 . H/PR: 'A:L).				
N/A	16-10-2019	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java				https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	
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
Weakness	Publish Date	CVSS	SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L).	Patch	NCIIPC ID
jre					
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security).	https://securi ty.netapp.com /advisory/nta p-20191017-	A-ORA-JRE- 041119/529
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
			Supported versions that	0001/	
			are affected are Java SE:		
			7u231, 8u221, 11.0.4 and		
			13; Java SE Embedded:		
			8u221. Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized read access		
			to a subset of Java SE, Java		
			SE Embedded accessible		
			data. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability can also		
			be exploited by using APIs		
			in the specified		
			Component, e.g., through a		
			web service which		
			supplies data to the APIs.		
			CVSS 3.0 Base Score 3.7		
			(Confidentiality impacts).		
			CVSS Vector:		
			(CVSS:3.0/AV:N/AC:H/PR:		
			N/UI:N/S:U/C:L/I:N/A:N).		
			CVE ID : CVE-2019-2894		
			GVE ID . GVE-2019-2074		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	A-ORA-JRE- 041119/530

CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:R/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2933 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that	
SE, Java SE Embedded product of Oracle Java SE (component: Networking).	
are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person 16-10-2019 2 6 A-OI A-OI	A-JRE- 19/531
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-	9-10

Weakness	Publish Date	CVSS	D	escriptior	n & CVE II	D	Pato	:h	NCIIP	C ID
			This vapply typical load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	andbox frulnerabe to Java of ally in second conditions of the second co	ility doe deploym rvers, the only trus e install trator). e 3.1 mpacts) :N/AC:H	es not tents, tat sted ed CVSS				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with a Kerbe Java S Embe vulne Java S additi Succes vulne unaut critica acces SE En data. vulne	erability in the second of the	nbedded acle Java Kerbero rsions the re Java S , 11.0.4 abedded attacked at	s SE s). at E: and d: bloit ker via aise tacks act his lt in o ete ava ole	https://sty.netapy/advisorp-201910001/	p.com ry/nta	A-ORA-) 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			sandbapplication application a	ally in clipoxed Jave cations of applets (in sted code omes from the candbox in andbox						
N/A	16-10-2019	5.8	Vulne SE pr SE (co Suppo are af 11.0.4 explo allow attack acces proto Java S of this result read a Java S and u to cau service	erability is oduct of omponer orted verefected and 13. It wilners is unauthor of the cols to cols a cols to cols a cols to col	in the Ja Oracle Ja Oracle Ja It: Hots It: Hots It: Hots It: Hots It: Hots Itiple Itip	lava Java Java Java Java Java Java Java	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-ORA- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIF	PC ID
			sandbapplid Java a that le untru that cointern Java so This vapply typical load a code by an 3.0 Ba (Conf Availa Vector (CVSS N/UI:	Vulnerability in the Java SE, Java SE Embedded						
N/A	16-10-2019	4.3	CVE ID: CVE-2019-2977 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this				https:// ty.netap /advison p-20191 0001/	p.com y/nta	A-ORA- 041119	•
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	D	escription	n & CVE II	D	Pato	:h	NCIIF	CID
			cause service Java S Ember vulne Java de typical sandhat le untru that control interrol Java son the Composite of the Composite of the Composite of the Composite of the CVSS (Available CVSS (CVSS N/UI:	chorized a partia ce (partia ce) (partia c	I denial al DOS) of E ote: This applies to ents, ents run le (e.g., com the rely on the for securility can by using degr, throw which to the A Score 3 mpacts) :N/AC:H ::N/I:N/	of of of sto nning Start oxed sE 8), code the rity. also APIs ugh a PIs. 5.7 . I/PR: A:L).				
N/A	16-10-2019	4.3	CVE ID: CVE-2019-2978 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to				https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-ORA- 041119	
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	D	escription	& CVE II)	Pato	h	NCIIP	C ID
			SE En attack vulne unaut cause service Java S Embe vulne Java d typica sandh applice Java a that le untru that c interregion Java s This very in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	romise Janbedded. Its of this rability of thorized a partial se (partial se (p	can resurability to denial al DOS) of E ote: This applies to ents, ents run e (e.g., com the rely on to for securality can y using deg, through to the Al Score 3 mpacts).	sful lt in o of of of aning Start oxed E 8), ode che rity. also APIs also APIs .7 .7 .7 .7 .7 .7 .7 .7 .7 .7 .7 .7 .7				
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221.				https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	
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	D	escription	n & CVE I	D	Pato	h	NCIIF	C ID	
Weakness	Publish Date	CVSS	Diffice vulner unaut comp SE En attack vulner unaut cause service Java S Ember vulner Java S Ember vulner that is interrupted to the Comp web s suppliced suppliced suppliced to the Comp web S suppliced S (CVSS (CVSS (CVSS)	escription all to expendent of the protocord and and and and and and and and and an	ploit allows and access to access the access to access the access to access the access the access the access to access t	eker via lava sful lt in co of of sconning Start oxed E 8), code the rity. also APIs also APIs7	Pato	ch .	NCIIF	PCID	
			Í	N/S:U/C D : CVE-							
N/A	16-10-2019	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: 2D). Supported versions that				https:// ty.netap /advisor p-20191	p.com y/nta	A-ORA-JRE-		
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	D	escription	& CVE II	D	Pato	h	NCIIP	CID
WEAKIIESS	rubiisii Date	CV33	are af 11.0.4 exploration allow attack access proto Java S of this result ability denial DOS) vulne Java de typical sandbe applied applied Java attack access proto Java S of this result ability denial DOS) vulne Java de typical sandbe applied Java attack access and be explicated at the Complete of the	fected ard 13. it vulner is unauth for with response in unauto to cause in unauto of Java Stations of Java S	re Java S Difficult ability enticate network diple omprom ssful att ability ca thorized e a parti ce (part E. Note: applies t ents rur va Web S r sandb n Java S r sandb n Java S run e (e.g., c om the rely on t for secu ility can y using d g., throughich to the A Score 3 mpacts) EN/AC:H EN/I:N/ 2019-2 in the Ja	EE: tto ed cacks an dial tial This to nning Start oxed E 8), code the rity. also APIs ugh a PIs7 . I/PR: A:L). 987 va	0001/		INCHIP	CID
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that				https://securi ty.netapp.com /advisory/nta p-20191017-		A-ORA- 041119	
CV Scoring Scal	le 0-1	1-2	2-3		4-5					

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			are affected are Java SE:	0001/	
			7u231, 8u221, 11.0.4 and		
			13; Java SE Embedded:		
			8u221. Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized ability to		
			cause a partial denial of		
			service (partial DOS) of		
			Java SE, Java SE		
			Embedded. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability does not		
			apply to Java deployments,		
			typically in servers, that		
			load and run only trusted		
			code (e.g., code installed		
			by an administrator). CVSS		
			3.0 Base Score 3.7		
			(Availability impacts).		
			CVSS Vector:		
			(CVSS:3.0/AV:N/AC:H/PR:		
			N/UI:N/S:U/C:N/I:N/A:L).		
			CVE ID : CVE-2019-2988		

Weakness Publish Date	CVSS	D	escription	ı & CVE II	D	Pat	ch	NCIIF	C ID
N/A 16-10-2019	4.3	Graal' Edition Graal' Java). version 19.2.0 vulne unaut with r multip comp: Graal' Edition vulne Graal' Edition signific additi Succe vulne unaut deleti access Oraclo Edition CVSS (Integ Vecto (CVSS N/UI:	5:3.0/AV: N/S:C/C	rprise act of Ora apponent: apported affected by affected attac access v ac	d is loit ker via cle his lt in or all prise a8 VSS	https://ty.netap/adviso.p-20193	p.com ry/nta	A-ORA- 041119	-
N/A 16-10-2019	4.3	CVE ID: CVE-2019-2989 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit				https://ty.netap/advisorp-20193	p.com ry/nta	A-ORA- 041119	-
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	D	escription	n & CVE II	D	Pato	:h	NCIIF	CID
Weakness	Publish Date	CVSS	vulne unaut with r multip comp SE En attack vulne unaut cause servic Java S Embe vulne Java d typica sandb applic Java a that le untru that c interr Java s This v apply typica load a code (by an 3.0 Ba (Avail CVSS N/UI: CVE I	rability and rability and run complets (in sed and and box and run complets (in sed administrations of the sed and run complets (in sed and run co	allows access to access to access to ava SE, J . Succes can resu ability t I denial al DOS) access can resu ability t I denial al DOS) access can resu ability t I denial al DOS) access can resu ability t I denial al DOS) access can resu ability t I denial al DOS) access can resu ability t I denial access applies t access access ability t access	eker via lava sful lt in to of of late of late of late of late oxed let entry. es not let ed late of late of late oxed let ed late oxed	https://	securi		
N/A	16-10-2019	4	SE, Java SE Embedded product of Oracle Java SE (component: Deployment). The				ty.netap /advisor p-20191	p.com cy/nta	A-ORA- 041119	
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
			supported version that is	0001/	
			affected is Java SE: 8u221;		
			Java SE Embedded: 8u221.		
			Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks require human		
			interaction from a person		
			other than the attacker.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Java SE, Java SE		
			Embedded accessible data		
			as well as unauthorized		
			read access to a subset of		
			Java SE, Java SE Embedded		
			accessible data. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability does not		
			apply to Java deployments,		
			typically in servers, that		
			load and run only trusted		
			code (e.g., code installed		
			by an administrator). CVSS		
			3.0 Base Score 4.2		
			J.J Dasc JCUI C T.Z		

9-10

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			Integrated Vector (CVSS N/UI:	identiali rity impa r: 5:3.0/AV R/S:U/C D : CVE- erability	ncts). CV :N/AC:H :L/I:L/ <i>F</i> 2019-2	/PR: A:N). 996				
N/A	16-10-2019	4	SE prosections SE (consumplinations) SE (consumplinations) Successive the second secon	erability of oduct of omponer orted vere fected and a chenticate of protocolor and the control of the control o	Oracle Jat: Javad rsions the Java St., 11.0.4 exploit allows red attactances while the sin Java gnificant cessful can resulupdate, access a read access a re	ava oc). at E: and ker via uire om a e a SE, atly lt in s to sible cess This co aning Start oxed	https://sty.netapy/advisorp-201910001/	p.com ry/nta	A-0RA-) 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			untru that c interr Java s This v apply typica load a code by an 3.0 Ba (Conf Integr Vecto (CVSS	oad and sted cod omes fromes from andbox andbox andbox and	le (e.g., com the rely on the for secuility doe deploymers, the only trusted trator). Le 4.7 ty and acts). CV	the rity. es not nents, nat sted ed CVSS				
			CVE I	D : CVE-	2019-2	999				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with a multi comp SE En attack vulne unaut deleti acces Java Sacces	erability ava SE Ence of Orace of Orace of Orace of Ence of En	nbedded acle Java Librarie Esions the Java S , 11.0.4 nbedded attacked attacked access vocols to ava SE, J . Succes can resurbed attacked	I a SE s). nat sE: and d: bloit ker via Java sful on or all dded This	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			typical sandbapplical sandbapp	deploymonally in clipoxed Jave Cations of applets (in oad and steed code and steed comes from the comes from the candbox of andbox of an	ents rur va Web S r sandb in Java S run le (e.g., c om the rely on t for secu ility can by using d leg., through to the A Score 5 eacts). C' EN/AC:H	Start oxed oxed EE 8), code the rity. also APIs ugh a PIs. 5.9 VSS				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with a multi comp SE En attack vulne unaut unaut unaut	erability and SE Emuct of Oraponent: 2 ponent: 2 ponent: 2 ponent: 2 ponent: 2 ponent: 2 ponenticate and the ple protocomise Judge of this erability of thorized apartia	nbedded acle Java 2D). rsions the Java S, 11.0.4 abedded attacked attacked access who cols to ava SE, J. Success can result to the success which is the success to ava SE, J. Success can result ability the success to a success can result ability the	l a SE nat SE: and d: cloit cker via fava sful	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-ORA- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			service Java S Ember vulne Java de typical sandh applice Java a that le untru that control interrest Java service This was a supple Competer Supple CVSS (Available CVSS (CVSS N/UI:	ce (partial E. Java Sedded. No rability a deployment of the correct of the correc	al DOS) SE ote: This applies a policy and Se or sandb in Java S run le (e.g., o om the rely on for secu olity can oy using ed .g., thro which to the A score 3 mpacts) :N/AC:H C:N/I:N/	of sto nning Start oxed SE 8), code the rity. also APIs ugh a PIs. 3.7 . I/PR: (A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Concu versice are Ja 11.0.4 Embe Diffice vulne unaut with a multip	erability va SE En oct of Ora ponent: ons that a va SE: 7 d and 13 dded: 8 orability a chenticat network ple proto romise J	nbeddedacle Java . Support are affect u231, 8t ; Java SE u221. ploit allows ted attact access to	ted cted u221, cker	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	A-ORA- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			attack vulne unaut cause service Java S Embe vulne explo data t specif withou Java V applie Java a throu CVSS (Avail CVSS (CVSS N/UI:	nbedded as of this rability of thorized a partial as (partial E, Java S and E, S and E	can resurability to ability to ability to ability to all DOS) of the appropriate to the appropriate to service as a servic	lt in of of of s be g ted sted c7 . I/PR: A:L).				
N/A	16-10-2019	4.3	CVE ID: CVE-2019-2964 Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to				https://sty.netapy/advisorp-20191	p.com ry/nta	A-ORA- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			service Java S Ember Vulne Java d typica sandh applice Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	a partia te (partia te (partia te, Java S dded. No rability a leployme ally in cli boxed Jav cations o applets (i boad and sted cod omes fro net) and andbox rulnerab ploited b specifie conent, e ervice w ies data 3.0 Base lability in Vector: 6:3.0/AV N/S:U/C D: CVE-	al DOS) EE ote: This applies tents, ents run le (e.g., of om the rely on for secu ility can by using d le (e.g., thro by to the A e Score 3 empacts) :N/AC:H C:N/I:N/	of sto nning Start oxed SE 8), code the rity. also APIs ugh a PIs. 3.7 . H/PR:				
N/A	16-10-2019	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java				https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	A-ORA- 041119	
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
			SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L).		
outside_in_te	chnology		0.2121012 2017 2710		
			Vulnerability in the Oracle		
N/A	16-10-2019	7.5	Outside In Technology product of Oracle Fusion Middleware (component:	N/A	A-ORA-OUTS- 041119/548
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
			Outside In Filters). The		
			supported version that is		
			affected is 8.5.4. Easily		
			exploitable vulnerability		
			allows unauthenticated		
			attacker with network		
			access via HTTP to		
			compromise Oracle		
			Outside In Technology.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Oracle Outside In		
			Technology accessible		
			data as well as		
			unauthorized read access		
			to a subset of Oracle		
			Outside In Technology		
			accessible data and		
			unauthorized ability to		
			cause a partial denial of		
			service (partial DOS) of		
			Oracle Outside In		
			Technology. Note: Outside		
			In Technology is a suite of		
			software development kits		
			(SDKs). The protocol and		
			CVSS score depend on the		
			software that uses the		
			Outside In Technology		
			code. The CVSS score		
			assumes that the software		
			passes data received over		
			a network directly to		
			Outside In Technology		
			code, but if data is not		
			received over a network		
			the CVSS score may be		
			lower. CVSS 3.0 Base Score		
			7.3 (Confidentiality,		

	Date CV	SS	D	escription	1 & CVE II	J	Pato	n	NCIIP	C ID
N/A 16-10-		I i i () M () () I i i i i i i i i i i i i i i i i i i	Integration packets of the control o	rity and Acts). CVS. 1:3.0/AV N/S:U/C D: CVE-rability and act of Oraceware (of the In Filtorted versed is 8.5 itable vursum authors via HT romise Code In Technology (act of the In Technology (act of t	Availabi S Vector :N/AC:L :L/I:L/A 2019-2 in the Or chnology acle Fusion that ters). The rsion that the action that the chnology acle Fusion that the component ters) and the chnology acle fusion that the chnology acks of the can resulupdate, the access	lity : /PR: A:L). 901 racle vion ent: e nt is / ity ed x his lt in	N/A	in .	A-ORA-0	OUTS-
10-10-	2019 7.3	t t t t t t t t t t t t t t t t t t t	data a unaut to a su Outsic access unaut cause Oracle Techn Tec software (SDKs CVSS &	as well as horized abset of de In Teosible dat horized a partial e Outside Chnology. No chnology are develon. The processore de la Teosible In Teosible CVS	read according of the control of the	cess of of tside te of t kits and the	IN/A		041119	/549
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	D	escription	& CVE II	D	Pa	tch	NCIIP	C ID
			passe a netw Outside code, receive the CV lower 7.3 (C) Integration (CVSS N/UI:	nes that to s data re work direct de In Tect but if da wed over VSS score CVSS 3. confident city and A cts). CVSS S:3.0/AVS N/S:U/C	ceived of ectly to chnology ta is not a network of Base Stality, Availabits Vector :N/AC:L	over y c ork e Score lity : /PR: A:L).				
N/A	16-10-2019	7.5	Outside production of the prod	erability in the In Tect of Oracle In Filt or ted versed is 8.5. itable vursed is with a via HTT romise Office In Tect of Oracle in Oracle in Section of Oracle in Tect of Ora	chnology acle Fus compon ters). The sion that 4. Easily lenticated network of the chnology acks of the can resulupdate, the accessible of the component of the chnology acks of the can resulupdate, the accessible of the component of the chnology and ability the denial	y ion ent: le at is y lity ed k this lt in le In e cess	N/A		A-ORA- 041119	
CV Scoring Sca	lo									

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
			Techn In Techn (SDKs) CVSS softw Outsi code. assum passe a netw Outsi code, receiv the C' lower 7.3 (C) Integration (CVSS) N/UI:	chnology are developed in Te cysnes that are that as data rowork direct de In Te but if dayed over CVSS 3 Confidentity and cts). CVS CS 3 CONFIDENTITY and CVS CS 3 CONFIDENTITY and CVS CS 3 CVS CS CS 3 CVS CS	Note: Ou y is a sui elopment protocol epend or uses the chnolog the soft eccived of chnolog ata is not e a netwo te may be	te of t kits and the e y ware over y tork e Score lity : /PR: A:L).				
N/A	16-10-2019	7.5	Outsi produ Middle Outsi suppo affect explo allow attack acces comp Outsi Succes vulne unaut insert	de In Te act of Or leware (de In Fil orted ve ed is 8.5 itable vu s unauth ker with romise (de In Te essful att rability thorized		ion ent: ent is y lity ed k chis chis	N/A		A-ORA- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
Weakness	Publish Date	CVSS	Technical data a unautito a si Outsidacces unauticause service Oracle Technical In Technical CVSS softworth outside code. assumpasse a networth outside code, receive the CV lower 7.3 (C) Integrating and (CVSS N/UI:	escription of the control of the con	ccessible of read according and ability to define the long of the software the soft	cess y to of of tside te of t kits and the e y ware over y cork e Score lity : /PR: A:L).	Pato	c'n e e e e e e e e e e e e e e e e e e e	NCIIP	CCID
N/A	16-10-2019	7.5	Vulne Outsid produ Middl Outsid suppo affect explo	erability in the de In Tector of Oracle ware (de In Filtorted versed is 8.5 itable vunauth	in the Ochnolog acle Fus compon ters). The sion that .4. Easily	racle y ion ent: e at is y	N/A		A-ORA- 041119	
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	D	escription	1 & CVE I	D	Pato	h	NCIIP	C ID
			attacl	ker with	networ	k				
			acces	s via HT	TP to					
			comp	romise (Oracle					
			Outsi	de In Te	chnolog	y.				
			Succe	essful att	acks of t	this				
			vulne	rability (can resu	ılt in				
			unau	thorized	update,					
			inser	t or delet	te acces	s to				
			some	of Oracl	e Outsid	le In				
			Techi	nology a	ccessible	е				
			data a	as well as	S					
			unau	thorized	read ac	cess				
			to a s	ubset of	Oracle					
			Outsi	de In Te	chnolog	v				
				sible dat	_					
			unau	thorized	ability t	.0				
				a partia	-					
				ce (partia						
				e Outsid	-					
				nology. N		tside				
				chnology						
				are deve						
				s). The p	_					
			-	score de						
				are that	_					
				de In Te						
				The CVS	U	9				
				nes that		ware				
				es data re						
			_	work dir		3 ()				
				de In Te	•	17				
				but if da						
				ved over						
				VSS scor						
				r. CVSS 3	•					
						Score				
			-	Confident	_	1:4				
			_	rity and .		-				
				cts). CVS						
			-	S:3.0/AV	-	-				
			N/UI:	:N/S:U/C	.:L/I:L/	A:LJ.				
			CVE I	D : CVE-	2019-2	971				
CV Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	Ŭ I			276			,			J 10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	7.5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not	N/A	A-0RA-0UTS-041119/553

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
			the CV lower 7.3 (C Integr impac (CVSS N/UI:	ved over VSS scor CVSS 3 Confiden rity and cts). CVS S:3.0/AV N/S:U/C	e may be not be tiality, Availabith S Vector of the time of time of the time of the time of the time of time of the time of time o	e Score lity :: ./PR: A:L).				
content_man	200r		CVLI	D. CVE	2017 2)				
N/A	16-10-2019	5	Conte of Orac (comp Suppo are af 12.1.3 Easily vulne unaut with the HTTP Oracl While in Orac Mana significated additional some Mana CVSS (Integ Vector (CVSS N/UI:	erability ent Mana acle E-Bo ponent: orted ve fected a 3 and 12 vexploit rability chenticat network to comple conter ethe vul acle Con ger, atta icantly i i	ger pro- usiness S Content rsions the re 12.1.2 able allows ted attack access we promise at Manage nerabilite tent cks may mpact oducts. acks of te can resulupdate, te access e Content sible da e Score 5 pacts). Content can Sible da e Score 5 pacts). Content can Sible da e Score 5	duct Suite). hat L- 2.9. cker via ger. ty is chis alt in s to nt ata. 6.8 VSS //PR: A:N).	N/A		A-0RA- 041119	
CV Scoring Sca	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
vm_virtualb	ox				
N/A	16-10-2019	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.34 and prior to 6.0.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 2.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR: H/UI:N/S:U/C:N/I:N/A:L).	N/A	A-ORA-VM_V- 041119/555
N/A	16-10-2019	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.34 and prior to 6.0.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM	N/A	A-ORA-VM_V- 041119/556

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pate	ch	NCIIP	CID
			comp Virtua vulne VM Vinay s additi Succe vulne unaut cause repea (comp VM Vinaut insert some Virtua and u acces Oracl acces (Conf and A CVSS (CVSS H/UI:	alBox extromise (alBox. Wrability in intualBox actional properties and and of the intualBox actional properties and intualBox actional properties to a sulfational properties to a sulfational properties to a sulfational properties alBox actional propert	Oracle V Thile the is in Oracle V Thile the is in Oracle X, attack of the cacks of the carrier of the cacks of the cack of the cac	M cle cs act chis clt in co ently acle l as d 3.0 grity cts). /PR: A:H).				
N/A	16-10-2019	2.1	VM Vi Oracl (comp Suppo are af 5.2.34 Easily vulne privil logon	erability irtualBoze Virtual ponent: (ported ver fected and and pri rexploits rability a eged atta to the in	x productivation Core). rsions the Prior for to 6.0 able allows heacker win	nat to 0.14. igh	N/A		A-ORA- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			comp Virtua vulne VM Vi may s additi Succe vulne unaut cause repea (comp VM Vi Base S (Avail CVSS (CVSS H/UI:	alBox exc romise (alBox. W rability in irtualBox significant ional pro- ssful atta- rability of table cra- plete DO irtualBox Score 6.0 lability in Vector: S:3.0/AV N/S:C/O						
N/A	16-10-2019	2.1	Vulne VM Vi Oracle (comp Suppo are af 5.2.34 Easily vulne privil logon where Virtua comp Virtua vulne VM Vi may s additi Succe	erability in tual Box erability and pring and pring ability and and pring albox exercity albox. We rability in tual Box exercity in tual Box exercity and property in tual Box exercity and property in tual Box exercity in the tual Box exercity in tual Box exercity in the tual Box exercity in tual Box exercity in tual Box exercity in tual Box exercity in t	in the Ox productive prior to 6.0 able allows he acker with the first to Oracle V. Thile the fis in Orack, attack attly impoducts. acks of the products.	racle ct of nat to 0.14. igh other of M cle s act	N/A		A-ORA- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
			cause repea (comp VM Vi Base i (Avail CVSS (CVSS H/UI:	chorized a hang of table cra plete DO irtualBox Score 6.0 lability in Vector: S:3.0/AV N/S:C/O D: CVE-	or frequency ash S) of Orax. CVSS: mpacts) :L/AC:L :N/I:N/	ently acle 3.0 . /PR: A:H).				
N/A	16-10-2019	2.1	VM Vioracli (composupped are aff 5.2.34 Easily vulner privil logon where Virtual composupped additional vulner vul	rability intual Box e Virtual Box orted verificated and pring a land pring of the interpretable of the intual Box exploit and pring intual Box explorized a hang of table crapilete DO intual Box Score 6.0 lability in Vector:	x productive prices to 6.0 able allows he acker with the firstruction or to 6.0 able allows he acker with the first to 6.0 acks of the can result ability the frequency of or frequency or fre	at to 0.14. igh ith cture of M cle is act in to ently acle 3.0	N/A		A-0RA-\ 041119	_
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	Pu	blish Date	cvss	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
				H/UI:	N/S:C/0	C:N/I:N/	A:H).				
				CVE I	D : CVE	-2019-3	005				
N/A	16-	10-2019	4.6	VM V Oracl (com) Supple are aff 5.2.34 Easily vulne privil logon wher Virtue vulne VM V may s addit Succe vulne takeo Virtue Score Integ impae (CVSS H/UI:	erability irtualBo e Virtual ponent: orted verected a 4 and provention of the control of the con	x produ lization Core). rsions tl re Prior ior to 6.0 able allows h acker w nfrastru VM ecutes t Oracle V rhile the is in Ora x, attack ntly imp oducts. racks of th can resu racle VM VSS 3.0 1 nfidentia Availabi S Vector C:L/AC:L	at to 0.14. ligh ith cture o M cle as act chis alt in H Base ality, ility c: /PR: A:H).	N/A		A-ORA- 041119	
N/A	16-	10-2019	2.1	VM V Oracl (com Supporare at 5.2.34 Easily	ulnerability in the Oracle M VirtualBox product of racle Virtualization component: Core). upported versions that re affected are Prior to 2.34 and prior to 6.0.14. asily exploitable ulnerability allows low					A-ORA- 041119	-
				vulne	rability	allows l	ow				
CV Scoring Sca	ale	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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
			logon where Virtus comp Virtus vulne VM V may s addit Succe vulne unaut cause repea (comp VM V Base (Avai CVSS (CVSS L/UI:	eged att to the in e Oracle alBox ex romise (alBox. W rability irtualBo significan ional pro essful att rability thorized a hang o irtualBo Score 6.! lability i Vector: S:3.0/AV N/S:C/C D: CVE-	nfrastructure VM ecutes to Oracle V hile the is in Orack, attack of the can result ability to freque ash OS) of Orack CVSS in mpacts) C:L/AC:L ::N/I:N/A	cture M cle s act chis clt in co ently acle 3.0 /PR: A:H).				
N/A 16-2	10-2019	2.1	VM V Oracl (composite of the composite o	erability irtualBo e Virtual ponent: orted ve fected a 4 and pri v exploit rability eged att to the in e Oracle alBox ex romise (alBox. W rability irtualBo significan	x production Core). rsions the Prior to 6.0 able allows loacker with the Coracle Value of the	nat to 0.14. ow ith cture M cle	N/A		A-ORA- 041119	
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
			additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR: L/UI:N/S:C/C:H/I:N/A:N). CVE ID: CVE-2019-3026		
N/A	16-10-2019	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.34 and prior to 6.0.14. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:	N/A	A-ORA-VM_V- 041119/563

Weakness	Publish	Date	CVSS	D	escription	n & CVE II	D	Pate	ch	NCIIP	C ID
				L/UI:	N/S:C/C	:H/I:H/	A:H).				
				CVE I	D : CVE-	2019-3	028				
N/A	16-10-2	2019	2.1	VM Vioracle (composupped are aff 5.2.34 Easily vulne privil logon where Virtual vulne VM Virtual vulne VM Virtual vulne	erability intualBone Virtual Bonent: 0 orted verificated and pring ability in a commise (albox exploits in a commise (albox) which are albox at a commise (albox) and properties and a commise (albox)	x productivation Core). rsions the re Prior for to 6.0 able allows heacker with the restruction Coracle V. Thile the ris in Oracle V. Thile the resurbidity importance of the resurbidity importance v. The resurbidity is v. The resurbidity in v. The resurbidity in v. The resurbidity in v. The resurbidity is v. The resurbidity in v. The resurbidity in v. The resurbidity is v. The resurbidity in v. The resurbidity is v. The resurbidity in v. The resurbidity in v. The resurbidity is v. The resurbidity is v. The resurbidity in v. The resurbidity is v. The resurbidity is v. The resurbidity in v. The resurbidity is	at to 0.14. igh ith cture of M cle is act of this of the condition of th	N/A		A-ORA-\\\041119	_
primavera_p	o_enter]	prise_]	rojec	_			111				
N/A	16-10-2	2019	3.5	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component:				N/A		A-ORA- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIF	C ID
Weakness	Publish Date	CVSS	Web A version are 17 exploration allow attack access to the person attack vulner access acces	Access). Ons that a 7.1.0-17. itable vurs itable vurs its itable vurs its itable itable vurs itable vu	Support are affect 12.12. Endinerability in the service of the ser	ted casily lity k ra P6 t. quire om a e e rise may chis clt in co ete a P6 t 3.0 cts). /PR: A:N).	Pato	ch Carlotte	NCIIF	PCID
N/A	16-10-2019	5.8	Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported				N/A		A-ORA- 041119	
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
			versions that are affected		
			are 15.1.0-15.2.18, 16.1.0-		
			16.2.18, 17.1.0-17.12.14		
			and 18.1.0-18.8.11. Easily		
			exploitable vulnerability		
			allows unauthenticated		
			attacker with network		
			access via HTTP to		
			compromise Primavera P6		
			Enterprise Project		
			Portfolio Management.		
			Successful attacks require		
			human interaction from a		
			person other than the		
			attacker and while the		
			vulnerability is in		
			Primavera P6 Enterprise		
			Project Portfolio		
			Management, attacks may		
			significantly impact		
			additional products.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized creation,		
			deletion or modification		
			access to critical data or all		
			Primavera P6 Enterprise		
			Project Portfolio		
			Management accessible		
			data as well as		
			unauthorized access to		
			critical data or complete		
			access to all Primavera P6		
			Enterprise Project		
			Portfolio Management		
			accessible data. CVSS 3.0		
			Base Score 9.3		
			(Confidentiality and		
			Integrity impacts). CVSS		
			Vector:		
			(CVSS:3.0/AV:N/AC:L/PR:		

Weakness	Publish Date	e CVSS	D	Description & CVE ID			Pato	h	NCIIP	C ID
			N/UI:	R/S:C/C	::H/I:H/	A:N).				
			CVE I	D : CVE-	2019-3	020				
database_ser	ver									
Improper Input Validation	16-10-2019	4.3	VM conditions and the state of	5:3.0/AV N/S:C/C D : CVE -	nt of Orazer. rsions the re 11.2.0 and 1.2.0 and 1.2.0 access to cave VM. access where the care to ducts. acks of the care to diffication cal data access to cave VM. access of the care to diffication cal data access to cave 6 access	at 0.4, and it cker via cy is ay chis lt in or all ta8 VSS	N/A		A-ORA- 041119	
Information Exposure	16-10-2019	4	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create				N/A		A-ORA- 041119	
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				Pato	:h	NCIIP	CID
			Session privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data. CVSS 3.0 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).							
			CVE I	D : CVE-	2019-2	913				
Information Exposure	16-10-2019	4	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS				N/A		A-ORA- 041119	
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
			Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:C/C:L/I:N/A:N). CVE ID: CVE-2019-2939			
Improper Input Validation	16-10-2019	2.1	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Create Session privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data. CVSS 3.0 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR: H/UI:N/S:U/C:N/I:L/A:N). CVE ID: CVE-2019-2940	N/A		A-ORA-DATA- 041119/570
N/A	16-10-2019	4	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create	N/A		A-ORA-DATA- 041119/571
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	D	escription	1 & CVE II	D	Pato	:h	NCIIP	C ID
			DBMS with r Oracle Core I attack vulne unaut insert some access Base S impac (CVSS L/UI:)		OR privi access vectors Success can resu update, te access RDBMS a. CVSS 3 (Integr S Vectors :N/AC:L	via nise ful lt in s to 3.0 rity : /PR: A:N).				
N/A	16-10-2019	3.3	L/UI:N/S:U/C:N/I:L/A:N). CVE ID: CVE-2019-2734 Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data and				N/A		A-ORA- 041119	
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
			cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR: L/UI:R/S:U/C:N/I:L/A:L). CVE ID: CVE-2019-2954		
N/A	16-10-2019	3.3	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:	N/A	A-ORA-DATA- 041119/573

Weakness	Publish Date	cvss	D	escription	ո & CVE I	D	Pato	:h	NCIIP	CID
			L/UI:	R/S:U/C	:N/I:L/ <i>I</i>	A:L).				
			CVE I	D : CVE-	2019-2	955				
N/A	16-10-2019	3.5	RDBM datab Oracle Support are af 12.2.0 Easily vulne privil Create with a multiple comp (jacks Succe huma perso attack vulne unaut cause repeat (comp RDBM datab Score impact (CVSS L/UI:	erability of MS (jacks ind) cone Databa orted verificated and D.1, 18c are exploited rability of exploited and interaction other facts of this rability of thorized a hang of table crapilete DO MS (jacks ind). CVS D: CVS	nponent ase Serversions the resions the resions to acker had access to cols to core RD bind). The results ability to request frequests for the results or frequests for the results of the	of er. nat D.2, ow aving ege via BMS quire om a er. alt in to ently re ase 7 cr. A:H).	N/A		A-0RA- 041119	
flexcube_dire	ect_banking			1 -2-		,				
N/A	16-10-2019	3.5	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component:				N/A		A-ORA- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			are 12 Easily vulne privile netwo to cor FLEXO Succe huma perso attack attack vulne unaut deleti access Oraclo Banki CVSS (Integ Vecto (CVSS L/UI:)	versions that are affected are 12.0.2 and 12.0.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 5.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:R/S:U/C:N/I:H/A:N).						
Information Exposure	16-10-2019	6.8	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: eMail). Supported versions that are affected are 12.0.2 and 12.0.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks of this			N/A		A-ORA- 041119		
						_				

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pato	h	NCIIP	C ID
			unaut critica acces FLEX acces Base (Conf CVSS (CVSS L/UI:	rability of thorized al data of second to the sible date of the sible of the si	access to rect Banka. CVSS ty impaction.	o ete king 3.0 cts). /PR: A:N).				
siebel_crm										
N/A	16-10-2019	5	Core Configuration Covers Configuration Covers Covers Configuration Covers Cove	erability - DB Dep guration e Siebel ponent: I guration ons that 9.8 and p itable vu s unauth s via HT romise S eployme guration cs of this rability chorized al data o s to all S eployme guration CVSS 3.0 Confiden cts). CVS S:3.0/AV N/S:U/O	oloymen produce CRM Install -). Support are affect orior. Eat all renticated network. The toological contraint access to acce	t and t of orted cted sily ity ed cted sily ed cted silver ed c	N/A		A-ORA-9 041119	
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			Pato	h	NCIIP	CID	
			CVE I	D : CVE-	2019-2	965				
business_inte	elligence_publ	isher	•							
N/A CV Scoring Sca	16-10-2019	5.8	Publis Oracl (composervice Service versice are 12 and 1 exploe allow attack acces comp (form Succe huma perso attack vulne Publis signifi additi Succe vulne unaut critica acces (form acces unaut insert some (form	erability is sher (for sher) proponent: It ce). Supponent: It ce). Suppons that a l.1.1.9.0, l.2.2.1.4.0 itable vu sunauth ser with ser with ser with ser and verability is sher (for sher), attained and the certain other to characterized and the left of BI Published at left of B	merly X oduct of Middles Mobile orted are affect 12.2.1 Easily linerabilitienticate network TP to BI Publis acks required than the while the sin BI merly X tacks man acks of the can result access the complete IP published as well access the can result access	ML ware cted 3.0 lity ed k sher her). juire om a e ML ay chis clt in co ete her her) l as s to her) 3.0	N/A		A-0RA- 041119	/578
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
marketing			Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2019-2906		
N/A	16-10-2019	5.8	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1- 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA- MARK- 041119/579

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2019-2994		
N/A	16-10-2019	5.8	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:	N/A	A-ORA- MARK- 041119/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N/UI:R/S:C/C:H/I:L/A:N).		
			CVE ID : CVE-2019-2995		
N/A	16-10-2019	5.8	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:H/I:L/A:N).	N/A	A-ORA- MARK- 041119/581

Weakness	Publish Date	cvss	Description & CVE ID	Pato	:h	NCIIP	CID
			CVE ID : CVE-2019-3000				
business_inte	elligence						
N/A CV Scoring Sca	16-10-2019	5.5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:	N/A		A-ORA-1 041119	
(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	Patc	h	NCIIP	C ID
			L/UI:N/S:C/C:L/I:L/A:N).				
			CVE ID : CVE-2019-2897				
Information Exposure	16-10-2019	5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:H/I:N/A:N). CVE ID: CVE-2019-2900	N/A		A-ORA-I 041119	
Information Exposure	16-10-2019	5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Installation). Supported versions that are affected are 12.2.1.3.0 and			A-ORA-I 041119	
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
			12.2.1 explo allow attack access comp Busin Enter the vu Orack Intelli Edition signif additi Succe vulne unaut critica access Busin Enter access Base S (Confi CVSS (CVSS N/UI:	itable vus unauth ser with so via HT' romise (cless Intelliprise Edulnerability of the control o	sily Ilnerabil Ienticate Inetworl IP to Oracle ligence ition. W Ity is in ss Interpris ss may Impact In the can resu Ity is in Ity impact Ity impa	hile e his lt in o ete 7.2. PR: A:N).				
N/A	16-10-2019	5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: BI Platform Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via			N/A		A-ORA- 041119		
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-3012							
annlication	object_library		CVEI	D:CAE.	-2019-3	012				
N/A	16-10-2019	5	Application Applic	Vulnerability in the Oracle Application Object Library product of Oracle E- Business Suite (component: Login Help). Supported versions that are affected are 12.2.5- 12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Object Library. CVSS 3.0 Base Score 5.3 (Availability impacts).					A-ORA- 041119	
CV Scoring Sca	ale 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
			(CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-3027		
istore			CVE 15 1 CVE 2017 3027		
N/A	16-10-2019	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Order Tracker). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:	N/A	A-ORA-ISTO- 041119/587

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N/UI:R/S:C/C:H/I:L/A:N).		
			CVE ID : CVE-2019-2990		
advanced_ou	itbound_teleph	ony			
N/A	16-10-2019	5.8	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data.	N/A	A-ORA-ADVA-041119/588

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2942		
hospitality_c	cruise_dining_r	oom_n	nanagement		
N/A	16-10-2019	5.5	Vulnerability in the Oracle Hospitality Cruise Dining Room Management product of Oracle Hospitality Applications (component: Web Service). The supported version that is affected is 8.0.80. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Dining Room Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Dining Room Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Dining Room Management accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-HOSP- 041119/589

Weakness	Publish Date	cvss	Description & CVE ID	Pa	itch	NCIIPC ID	
			(CVSS:3.0/AV:N/AC:L/P:L/UI:N/S:U/C:H/I:L/A:N CVE ID : CVE-2019-295	i).			
data_integra	tor	T					
N/A	16-10-2019	4	Vulnerability in the Oracle Data Integrator product Oracle Fusion Middlewar (component: Studio). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTF to compromise Oracle Data Integrator. Successification attacks of this vulnerability can result is unauthorized access to critical data or complete access to all Oracle Data Integrator accessible data CVSS 3.0 Base Score 6.5 (Confidentiality impacts CVSS Vector: (CVSS:3.0/AV:N/AC:L/PL/UI:N/S:U/C:H/I:N/A:NCVE ID: CVE-2019-294	of re e s s s s s s s s s s s s s s s s s		A-ORA-DATA- 041119/590	
food_and_be	verage_applica	tions					
N/A	16-10-2019	5.5	Vulnerability in the Orac Hospitality Reporting an Analytics component of Oracle Food and Beverag Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Inventor	ge N/A		A-ORA-F00D- 041119/591	
CV Scoring Sca (CVSS)	o-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9 9-10	

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			netwo to cor Hospi Analy attack vulne unaut critica access Hospi Analy as we updat access Hospi Analy CVSS (Conf Integr Vecto (CVSS L/UI:	ration proof access access of this rability Repaired and at a constant of the second access to all Optical type access to some	ess via HT ee Oracle eporting cessful can resu access t r comple exacte eporting essible d uthorize or dele e of Ora eporting essible d exacte cor dele exacte exac	e and ata ed te and ata. '.1 (SS //PR: A:N).				
Incorrect Authorizatio n	16-10-2019	5.8	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker				N/A		A-ORA- 041119	
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
			and while the vulnerability is in Oracle Hospitality Reporting and Analytics, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:L/I:L/A:N).		
bi_publisher					
Information Exposure	16-10-2019	4	Vulnerability in the BI Publisher (formerly XML Publisher) product of Oracle Fusion Middleware (component: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher).	N/A	A-ORA-BI_P- 041119/593

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
graalvm			Successful attacks of this vulnerability can result in unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2898		
			Vulnerability in the Oracle		
N/A	16-10-2019	4	GraalVM Enterprise Edition product of Oracle GraalVM (component: LLVM Interpreter). The supported version that is affected is 19.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.0 Base	N/A	A-0RA-GRAA- 041119/594

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
Weakness N/A	Publish Date	4.3	Score impact (CVSS L/UI: CVE I Vulne Graal Java). versical 19.2.0 vulne unaut with multi comp Graal Edition vulne Graal Editio	escription 7.7 (Ava cts). CVS S:3.0/AV N/S:C/C D: CVE- erability VM Ente on produ VM (com The sup on that is D. Difficu erability a thenticat network ple proto romise (VM Ente on. While erability i thenticat ional prote erability i thenticat ional prote crability i thenticat ional prote erability i thenticat i	initability S Vector :N/AC:L :N/I:N/A :2019-2 in the O rprise act of Ora inponent ported s affecte lt to exp allows access v ocols to Oracle rprise e the is in Ora rprise s may impact oducts. acks of t can resu odificati cal data	racle acle chis clt in n, on or all	https://ty.netap/advisorp-201910001/	securi p.com ry/nta	A-ORA-041119	GRAA-
			Edition CVSS (Integrated Vector (CVSS)	on access 3.0 Base grity imp	sible dat Score 6 pacts). C' :N/AC:H	a. 5.8 VSS I/PR:				
<i>c</i> . 11			CVE I	D : CVE-	2019-2	989				
field_service			₹71 -	makili.	: a + l - 0	ma el e				
Improper Authenticati	16-10-2019	4.3		erability Service p			N/A		A-ORA-	FIEL-
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
on			Oracle E-Business Suite (component: Wireless). Supported versions that are affected are 12.1.1- 12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Field Service. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Field Service, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Field Service accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:N/I:L/A:N). CVE ID: CVE-2019-2930		041119/596
siebel_ui_frai	mework				
Information Exposure	16-10-2019	5	Vulnerability in the Siebel UI Framework product of Oracle Siebel CRM (component: EAI). Supported versions that are affected are 19.8 and prior. Easily exploitable vulnerability allows	N/A	A-ORA-SIEB- 041119/597
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 363	6-7 7-8	8-9 9-10

unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel UI Framework access ble data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0)AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2935 retail_xstore_point_of_service Vulnerability in the Oracle Retail Xstore Point of Service product of Oracle Retail Applications (component: Point of Sale). Supported versions that are affected are 17.0.3, 18.0.1 and 19.0.0. Difficult to exploit vulnerability allows physical access to compromise Oracle Retail Xstore Point of Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Xstore Point of Service accessible data as well as	Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
Pretail_xstore_point_of_service Vulnerability in the Oracle Retail Xstore Point of Service product of Oracle Retail Applications (component: Point of Sale). Supported versions that are affected are 17.0.3, 18.0.1 and 19.0.0. Difficult to exploit vulnerability allows physical access to compromise Oracle Retail Xstore Point of Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Xstore Point of Service.				with network access via HTTP to compromise Siebel UI Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel UI Framework accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N).							
Vulnerability in the Oracle Retail Xstore Point of Service product of Oracle Retail Applications (component: Point of Sale). Supported versions that are affected are 17.0.3, 18.0.1 and 19.0.0. Difficult to exploit vulnerability allows physical access to compromise Oracle Retail Xstore Point of Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Xstore Point of Service				CVE I	D : CVE	-2019-2	935				
	N/A	16-10-2019	2.6	Retail Service Retail (composed Sale). That a 17.0.3 Diffice vulner physic composed Successive attack attack vulner unautinser some Xstor	Vulnerability in the Oracle Retail Xstore Point of Service product of Oracle Retail Applications (component: Point of Sale). Supported versions that are affected are 17.0.3, 18.0.1 and 19.0.0. Difficult to exploit vulnerability allows physical access to compromise Oracle Retail Xstore Point of Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail						

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Retail Xstore Point of Service accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:H/PR: H/UI:R/S:U/C:L/I:L/A:N). CVE ID: CVE-2019-2872		
forms					
N/A	16-10-2019	5.8	Vulnerability in the Oracle Forms product of Oracle Fusion Middleware (component: Services). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Forms. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Forms, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Forms accessible data as well as unauthorized read access to a subset of Oracle	N/A	A-ORA-FORM- 041119/599

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
			CVSS (Conf Integ Vecto (CVSS N/UI:	s accessing and accessing accession	e Score 6 ity and acts). CV ::N/AC:L	5.1 /SS ./PR: A:N).				
enterprise_m	ıanager									
N/A	16-10-2019	6	Enter Exada Enter (comply Plug-Supper and 13.2.2 13.3.2 explos allow attack access comply Mana Succes vulned takeo Mana 3.0 Bar (Confi and A CVSS (CVSS L/UI:	erability rprise Ma ata produprise Ma ponent: In Deplo orted ve ffected a 2.0.0, 13. 2.0.0. Diff it vulner is low pr ker with s via HT oromise I ger for H essful att erability ver of En ger for H ase Score identiality vector: 5:3.0/AV N/S:U/C D: CVE-	anager fouct of Oranager Exadata y and Interpretations the 12.1.0 are ficult to rability ivileged network Exadata. acks of the can resunterprise Exadata. te 7.5 aty, Integrate imparise Exadata. te 7.5 aty imparise Exadata. te 7.5 aty imparise Exadata.	cacle as). nat 0.5.0, and k se chis alt in e CVSS grity cts). H/PR: A:H).	N/A		A-ORA-1 041119	
micros_relate	e_customer_r	elation	nship_management_software							
N/A	16-10-2019	4.3	Vulnerability in the MICROS Relate CRM						A-ORA-1 041119	
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	NCIIPC ID
			Software product of Oracle Retail Applications (component: Internal Operations). Supported versions that are affected are 7.1.0, 15.0.0, 16.0.0, 17.0.0, and 18.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS Relate CRM Software. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MICROS Relate CRM Software accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:H/I:N/A:N). CVE ID: CVE-2019-2896		
annlication of	levelopment_f	rameu			
N/A	16-10-2019	3.5	Vulnerability in the Oracle JDeveloper and ADF product of Oracle Fusion Middleware (component: OAM). Supported versions that are affected are 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle	N/A	A-ORA-APPL- 041119/602

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			JDeveloper and ADF. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle JDeveloper and ADF accessible data. CVSS 3.0 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: H/UI:R/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2899		
N/A	16-10-2019	7.5	Vulnerability in the Oracle JDeveloper and ADF product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle JDeveloper and ADF. Successful attacks of this vulnerability can result in takeover of Oracle JDeveloper and ADF. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:	N/A	A-ORA-APPL- 041119/603

Weakness	Publish Date	CVSS	D	escription	escription & CVE ID			ch	NCIIP	CID
			N/UI:	N/S:U/C	:H/I:H/	A:H).				
			CVE I	D : CVE-	2019-2	904				
jdeveloper										
N/A	16-10-2019	3.5	JDeve produ Middle OAM) that a 11.1.1 12.1.3 Easily vulne privil network to con JDeve Succe huma perso attack vulne unaut to a st JDeve access Base S (Confi CVSS (CVSS H/UI: CVE I	rability floper an act of Ora eware (of Suppor re affect 1.9.0, 11. 3.0.0 and rexploits rability acts of this rability of thorized abset of loper an sible dat Score 2.4 identiality of the core acts of the core	d ADF acle Fus componented versed are 1.2.4.0, 12.2.1.3 able allows hacker with acker with acker with acker with an the essful can result acceptant acceptan	ion ent: sions 3.0. igh ith fTP e quire om a lt in cess 3.0 cts). /PR: A:N).	N/A		A-ORA- 041119	
N/A	16-10-2019	7.5	Vulnerability in the Oracle JDeveloper and ADF product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0				N/A		A-ORA- 041119	
CV Scoring Sc	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Desc	ription	& CVE II	D	Pato	h	NCIIP	CID
			and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle JDeveloper and ADF. Successful attacks of this vulnerability can result in takeover of Oracle JDeveloper and ADF. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:H/I:H/A:H). CVE ID: CVE-2019-2904							
web_services	5		CVL ID.	CVL	2017 2	JUT				
N/A	16-10-2019	6.4	Vulnerability in the Oracle Web Services product of Oracle Fusion Middleware (component: SOAP with Attachments API for Java). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Services. While the vulnerability is in Oracle Web Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update,				N/A		A-0RA- 041119	
CV Scoring Sca	ole 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
			insert or delete access to some of Oracle Web Services accessible data as well as unauthorized read access to a subset of Oracle Web Services accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:L/I:L/A:N). CVE ID: CVE-2019-2907		
workflow			GVE 10 : GVE 2017 2707		
N/A	16-10-2019	4.3	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Worklist). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Workflow accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:	N/A	A-ORA- WORK- 041119/607

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
			N/UI:R/S:U/C:N/I:L/A:N).						
			CVE ID : CVE-2019-2925						
hyperion_dat	ta_relationship	_mana	ngement						
N/A	16-10-2019	4.6	Vulnerability in the Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and Security). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Data Relationship Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Hyperion Data Relationship Management. CVSS 3.0 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: H/UI:R/S:U/C:H/I:H/A:H). CVE ID: CVE-2019-2927	N/A	A-ORA-HYPE- 041119/608				
nyperion_ent	hyperion_enterprise_performance_management_architect								
N/A	16-10-2019	3.6	Vulnerability in the Hyperion Enterprise Performance Management Architect product of Oracle Hyperion (component: Workspace).	N/A	A-ORA-HYPE- 041119/609				
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
			The supported version		
			that is affected is 11.1.2.4.		
			Difficult to exploit		
			vulnerability allows high		
			privileged attacker with		
			network access via HTTP		
			to compromise Hyperion		
			Enterprise Performance		
			Management Architect.		
			Successful attacks require		
			human interaction from a		
			person other than the		
			attacker and while the		
			vulnerability is in		
			Hyperion Enterprise		
			Performance Management		
			Architect, attacks may		
			significantly impact		
			additional products.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Hyperion		
			Enterprise Performance		
			Management Architect		
			accessible data as well as		
			unauthorized read access		
			to a subset of Hyperion		
			Enterprise Performance		
			Management Architect		
			accessible data. CVSS 3.0		
			Base Score 4.0		
			(Confidentiality and		
			Integrity impacts). CVSS		
			Vector:		
			(CVSS:3.0/AV:N/AC:H/PR:		
			H/UI:R/S:C/C:L/I:L/A:N).		
			CVE ID : CVE-2019-2941		
peoplesoft_e	nterprise_hum	an_cap	pital_management_human_r	resources	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	4	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: US Federal Specific). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PRL/UI:N/S:U/C:L/I:N/A:N) CVE ID: CVE-2019-2951		A-ORA-PEOP- 041119/610
hyperion_fin	ancial_reporti	ng			
N/A	16-10-2019	2.1	Vulnerability in the Hyperion Financial Reporting product of Oracle Hyperion (component: Security Models). The supported version that is affected is 11.1.2.4. Difficult to explo vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion	N/A	A-ORA-HYPE- 041119/611
CV Scoring Sca	le 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
			Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Hyperion Financial Reporting accessible data. CVSS 3.0 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: H/UI:R/S:U/C:N/I:H/A:N).		
neonlesoft e	nterprise_scm	enroc	CVE ID : CVE-2019-2959		
Information Exposure	16-10-2019	5	Vulnerability in the PeopleSoft Enterprise SCM eProcurement product of Oracle PeopleSoft (component: eProcurement). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible	N/A	A-ORA-PEOP- 041119/612

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-3001		
banking_digi	ital_experience	9			
Incorrect Authorizatio n	16-10-2019	4.9	Vulnerability in the Oracle Banking Digital Experience product of Oracle Financial Services Applications (component: Loan Calculator). Supported versions that are affected are 18.1, 18.2, 18.3 and 19.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Digital Experience. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Digital Experience, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Digital Experience accessible data as well as unauthorized read access to a subset of Oracle	N/A	A-ORA-BANK- 041119/613

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Banking Digital Experience accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:R/S:C/C:L/I:L/A:N). CVE ID: CVE-2019-3019		
installed_bas	se				
N/A	16-10-2019	4.3	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Engineering Change Order). Supported versions that are affected are 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector:	N/A	A-ORA-INST- 041119/614

Weakness	Publish D	Date	CVSS	D	escriptio	on & CVE ID		Pate	:h	NCIIF	PC ID
				`	S:3.0/AV	•	•				
				N/UI:R/S:C/C:N/I:L/A:N). CVE ID : CVE-2019-3024							
hospitality_r	es 3700			CVLI	D. CVE	2017 3					
N/A	16-10-20	019	6.8	Hospicompand B Application allow attack access compand B While in Ora 3700 signification addition and A CVSS (CVSS N/UI:	erability rational property it vulner of the	ES 3700 f Oracle The rsion that cability nenticate network TP to Oracle ES 3700 nerability may mpact oducts. acks of the can resuracle ES 3700 e Score 9 ity, Integrity impa	Food at is lt to ed k ty is RES this alt in . O.0 grity cts). H/PR: (A:H).	N/A		A-ORA- 041119	
weblogic_ser Information Exposure	16-10-20)19	4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported			N/A		A-ORA- 041119		
CV Scoring Sca (CVSS)	ale 0-1		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:U/C:L/I:N/A:N).							
Information Exposure	16-10-2019	5	Vulne WebL of Ora Middl EJB C version are 10 and 1 explon allow attack access comp WebL Succes vulne unaut to a si	attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server		N/A		A-ORA- 041119		
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			(Conf CVSS (CVSS N/UI:	Score 5.3 identiali Vector: 5:3.0/AV N/S:U/C D: CVE - erability	ty impa :N/AC:L ::L/I:N/. 2019-2	/PR: A:N). 888				
N/A	16-10-2019	5.8	WebI of Orac Middle Samp support affects Easily vulner unauth with the HTTF Oracl Successive WebI may stand inserts some Server well a access Oracl access Bases (Conf.)	legic Seracle Fusialeware (colle apps). Orted versed is 12. Or exploitation of the residual processful attainment of the rability of the or delete of Oracles to a sulper WebLock of Score 6.1 Tidentialiarity imparticularity	ver procon compon The rsion that 2.1.3.0. able allows access very acks requestion from than the ver, attained and the control of the control	ent: et is eker via er. quire om a e cle acks act chis lt in s to ogic a as read rer 3.0	N/A		A-ORA- 041119	
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	Patc	h	NCIIP	C ID
			(CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:L/I:L/A:N). CVE ID : CVE-2019-2889				
N/A	16-10-2019	6.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: H/UI:N/S:U/C:H/I:H/A:H).	N/A		A-ORA-V 041119	
N/A	16-10-2019	6.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to	N/A		A-ORA-\ 041119	
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	NCIIPC ID
			compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:H/I:H/A:H). CVE ID: CVE-2019-2891		
hospitality_r	eporting_and_	analyti	cs		
N/A	16-10-2019	5.5	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Admin - Configuration privilege with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle	N/A	A-ORA-HOSP- 041119/621

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pa	itch	NCIIP	C ID
			Analy CVSS (Conf Integ Vector (CVSS L/UI:	itality Revices accessories ac	essible descretes Score 8 sty and sacts). CV s:N/AC:L:H/I:H/	ata. 3.1 /SS ./PR: A:N).				
N/A	16-10-2019	4.9	Hosp Analy Oracl Appli suppo affect to exp allow attacl Confi with HTTF Oracl Repo Succe vulne unau deleti acces Oracl Repo acces unau critic acces Hosp Analy Confi	itality Revitics come e Food a cations. orted versed is 9.1 ploit vuling artion and extended at thorized at thorized at data of s to all Control and as to all Control and as to all Control and as to all Control and all data of s to all da	eporting aponent and Bever The rision that a.0. Difficing Administration and the careation odification ality acks of the careation odification ality and Analytica as well access the careation of the careation o	and of erage at is cult by a contact in a contact ics. It in a contact ics and a contact ics and a contact ics.	N/A		A-ORA- 041119	
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
Weakness N/A	Publish Date	5.5	CVSS:3.0/AV:N/AC:H/PR: L/UI:N/S:U/C:H/I:H/A:N). CVE ID: CVE-2019-2936 Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Admin - Configuration privilege with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS	Patch N/A	A-ORA-HOSP-041119/623
peoplesoft e	nterprise_peo	pletool	Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: L/UI:N/S:U/C:H/I:H/A:N). CVE ID: CVE-2019-2937		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Fluid Core). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:L/I:L/A:N). CVE ID: CVE-2019-2915	N/A	A-ORA-PEOP- 041119/624

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:L/I:L/A:N). CVE ID: CVE-2019-2929	N/A	A-ORA-PEOP- 041119/625

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:L/I:L/A:N). CVE ID: CVE-2019-2931	N/A	A-ORA-PEOP- 041119/626

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pate	ch	NCIIP	C ID
N/A	16-10-2019	4	People People Oracle (composition of the composition of the compositio	erability in leSoft En leTools per People ponent: I ger). Suppose that a solution of the People of the vulnional propersional propersional propersional propersional propersional propersional data on sto all People of the vulnional propersional propersi	terprise product of Soft Free ported are affect are affect are affect are affect are affect by leged network FP to PeopleToo nerabilit Enterpriattacks re access to can resu access to c	of cted sily lity k oft ols. cy is ise may chis elt in co ete ft ols 3.0 cts).	N/A		A-0RA- 041119	
N/A	16-10-2019	5.8	Peopl Peopl Oracle (comp Suppo are af 8.57.1	erability in the Soft Ender People: ponent: I ported verage Easily expression of the Easily expression of the Easily expension of the Easily expression of the Easily expre	terprise roduct Soft Fluid Co rsions the re 8.56 a	of re). nat and	N/A		A-ORA- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIII	PC ID
			unaut with a HTTP Peopl attack intera other and wis in F Peopl signification and with additional some Enter access unaut to a signification as a signification and with a significant access unaut to a significant acce	thenticate network of to compessor equiraction from the control of the control of Peoples of People	ted attack access to promise sterprise Successform a period attacks of the cattacks of the cat	cker via ful n rson er bility prise nay chis lt in s to els l as cess oft els 3.0				
N/A	16-10-2019	5.8	Peopl Peopl Oracle (comp Monit versionare 8. explo	erability eSoft En eTools p e People ponent: l tor). Sup ons that a itable vu s unauth	terprise product of Soft Perform ported are affect 3.57. Eas	of ance cted sily lity	N/A		A-ORA- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			acces comp Enter Succe huma perso attack vulne Peopl signif addit Succe vulne unaut insert some Enter acces unaut to a s Enter acces Genf Integ Vecto (CVSS N/UI:	cer with so via HT aromise It prise Person other and with a control of People of Peopl	TP to PeopleSo opleToo acks req ction fro than the while the is in atterprise acks of t can resu update, te access leSoft opleToo a as wel read acc PeopleS opleToo a. CVSS 1 atty and acts). CV	oft ols. quire om a e e may chis clt in s to ols cl as cess oft ols 3.0				
N/A	16-10-2019	4	Peopl Peopl Oracl (comp Broke version are 8.	erability leSoft En leTools p e People ponent: ler). Supp ons that s 56 and 8 itable vu	oroduct oroduct oroft Integrat oorted are affed 3.57. Eas ulnerabil	of ion cted sily lity	N/A		A-ORA- 041119	
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	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			access comp Enter Succe vulne unaut to a si Enter access (Conf CVSS (CVSS L/UI:	ker with s via HTZ romise Februse People ssful attached abset of a prise People sible datactions and the state of the stat	TP to PeopleSo popleToo acks of t can resu read acc PeopleS opleToo a. CVSS ty impac :N/AC:L :L/I:N/A	oft ols. his lt in cess oft ls 3.0 cts). /PR: A:N).				
			Vulne	erability i	in the					
N/A	16-10-2019	4.3	Oracle (comp Support are af 8.57. vulne unaut with a HTTP Peopl attack interation other and wis in F Peopl significated additional context and which is in F Peopl significated with a succession of the successio	eTools pe People ponent: Sorted verificated and Easily extrability at the etwork of the eTools. So requirection from the etwork of etwork of the etwork of the etwork of the etwork of etwork	Soft Styleshersions the electric staces where the staces of the contract of th	et). nat nd e ker via ful n rson er bility prise may	N/A		A-ORA- 041119	
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
			insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:R/S:C/C:N/I:L/A:N).		
Paloaltonetw	vorks		CVE ID : CVE-2019-3023		
globalprotec					
Improper Privilege Managemen t	16-10-2019	2.1	A Local Privilege Escalation vulnerability exists in the GlobalProtect Agent for Windows 5.0.3 and earlier, and GlobalProtect Agent for Windows 4.1.12 and earlier, in which the auto- update feature can allow for modification of a GlobalProtect Agent MSI installer package on disk before installation. CVE ID: CVE-2019- 17435	https://securi tyadvisories.p aloaltonetwor ks.com/Home /Detail/197	A-PAL-GLOB- 041119/632
Improper Privilege Managemen t	16-10-2019	6.6	A Local Privilege Escalation vulnerability exists in GlobalProtect Agent for Linux and Mac OS X version 5.0.4 and earlier and version 4.1.12 and earlier, that can allow non-root users to overwrite root files on the file system. CVE ID: CVE-2019- 17436	https://securi tyadvisories.p aloaltonetwor ks.com/Home /Detail/200	A-PAL-GLOB- 041119/633

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				Pato	:h	NCIIP	C ID
Philips											
intellispace_	perinata	l									
Exposure of Resource to Wrong Sphere	25-10-2	2019	7.2	Version vulner Intellication applied could unauth plocked or an deskt applied out from the accession with possible attack to escential to escential to escential vulner accession to possible attack to escential vulner accession to escential vulner accession to escential vulner accession to escential vulner accession vulner accession to escential vulner accession to escential vulner accession vul	In IntelliSpace Perinatal, Versions K and prior, a vulnerability within the IntelliSpace Perinatal application environment could enable an unauthorized attacker with physical access to a locked application screen, or an authorized remote desktop session host application user to break- out from the containment of the application and access unauthorized resources from the Windows operating system as the limited- access Windows user. Due to potential Windows vulnerabilities, it may be possible for additional attack methods to be used to escalate privileges on the operating system. CVE ID: CVE-2019-					A-PHI-II 041119	
PHP											
php											
Out-of- bounds Write	28-10-2	2019	7.5	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated			below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to php.net/bug.p hp?id=78599, https://suppo rt.f5.com/csp /article/K754 08500?utm_s				
CV Scoring Sca (CVSS)	lle 0-	-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIF	PC ID
			reser data,	rs into the ved for Forther thus oper this bility of section.	CGI pro	tocol e	ort&amj _mediun			
			CVE I 1104	D : CVE-	2019-					
Pivotal										
reactor_netty	7									
Insufficientl y Protected Credentials	17-10-2019	5	version passes redired author remo malicular access differ have	al Reactors prior es header ects, including the unautorious users to creducent servaccess to the contractors to the ent servaccess to the contractors to the ent servacces to the contractors to the contractors to the ent servacces to the ent	r to 0.8.2 through ones. A hentical r may galentials for than and the control of	l 1, gh ted ain for a	https:// l.io/secu ve-2019 11284	rity/c	A-PIV-F 041119	_
			1128	4						
pivotal_softw										
cloud_foundr	y_uaa		Cloud	l Foundr	τ, ΙΙΛ Λ		T .		l .	
Information Exposure	23-10-2019	4	Cloud Foundry UAA, versions prior to v74.3.0, contains an endpoint that is vulnerable to SCIM injection attack. A remote authenticated malicious user with scim.invite scope can craft a request with malicious content which can leak information about users of the UAA. CVE ID: CVE-2019-11282				https:// cloudfou org/blog 2019-11	undry. g/cve-	A-PIV-0 041119	
rabbitmq							•		•	
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	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Pivotal RabbitMQ, versions prior to v3.7.18, and RabbitMQ for PCF, versions 1.15.x prior to 1.15.13, versions 1.16.x prior to 1.16.6, and versions 1.17.x prior to 1.17.3, contain two components, the virtual host limits page, and the federation management UI, which do not properly sanitize user input. A remote authenticated malicious user with administrative access could craft a cross site scripting attack that would gain access to virtual hosts and policy management information. CVE ID: CVE-2019-11281				https:// l.io/secu ve-2019 11281	rity/c	A-PIV-R 041119	
Information Exposure	23-10-2019	ent 4	version contains vultinject auther user with a which information the U.	Cloud Foundry UAA, versions prior to v74.3.0, contains an endpoint that is vulnerable to SCIM injection attack. A remote authenticated malicious user with scim.invite scope can craft a request with malicious content which can leak information about users of the UAA. CVE ID: CVE-2019-				www. indry. g/cve- 282	A-PIV-0 041119	
Information Exposure	23-10-2019	4	Cloud Foundry SMB Volume, versions prior to			r to	https://cloudfou		A-PIV-C	LOU-
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	Pul	olish Date	cvss	Description & CVE ID			Patch		NCIIPC ID		
Through Log Files				v2.0.3, accidentally outputs sensitive information to the logs. A remote user with access to the SMB Volume logs can discover the username and password for volumes that have been recently created, allowing the user to take control of the SMB Volume. CVE ID: CVE-2019-11283			org/blog 2019-11		041119	/640	
cloud_foundry_smb_volume											
Information Exposure Through Log Files	23-	10-2019	4	Cloud Foundry SMB Volume, versions prior to v2.0.3, accidentally outputs sensitive information to the logs. A remote user with access to the SMB Volume logs can discover the username and password for volumes that have been recently created, allowing the user to take control of the SMB Volume. CVE ID: CVE-2019- 11283			https://www. cloudfoundry. org/blog/cve- 2019-11283		A-PIV-CLOU- 041119/641		
Postgresql											
postgresql											
Information Exposure	29-10-2019 3.		3.5	Postgresql, versions 11.x before 11.5, is vulnerable to a memory disclosure in cross-type comparison for hashed subplan. CVE ID: CVE-2019-10209			https://bugzil la.redhat.com /show_bug.cgi ?id=CVE- 2019-10209, https://www. postgresql.org /about/news/		A-POS-POST- 041119/642		
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Proftpd proftpd Loop with Unreachable Exit Condition ('Infinite Loop') Python python Improper Neutralizati on of Special Elements in Output Used	-10-2019	5	ProFTPD before 1.3.6b and 1.3.7rc before 1.3.7rc2 allows remote unauthenticated denial-of- service due to incorrect handling of overly long commands because main.c in a child process enters an infinite loop. CVE ID: CVE-2019- 18217 An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib	N/A	A-PRO-PROF- 041119/643
Loop with Unreachable Exit Condition ('Infinite Loop') Python python Improper Neutralizati on of Special Elements in	-10-2019	5	and 1.3.7rc before 1.3.7rc2 allows remote unauthenticated denial-of- service due to incorrect handling of overly long commands because main.c in a child process enters an infinite loop. CVE ID: CVE-2019- 18217 An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib	N/A	
Loop with Unreachable Exit Condition ('Infinite Loop') Python python Improper Neutralizati on of Special Elements in	-10-2019	5	and 1.3.7rc before 1.3.7rc2 allows remote unauthenticated denial-of- service due to incorrect handling of overly long commands because main.c in a child process enters an infinite loop. CVE ID: CVE-2019- 18217 An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib	N/A	
Unreachable Exit Condition ('Infinite Loop') Python python Improper Neutralizati on of Special Elements in	-10-2019	5	and 1.3.7rc before 1.3.7rc2 allows remote unauthenticated denial-of- service due to incorrect handling of overly long commands because main.c in a child process enters an infinite loop. CVE ID: CVE-2019- 18217 An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib	N/A	
Improper Neutralizati on of Special Elements in			urllib2 in Python 2.x through 2.7.17 and urllib		
Improper Neutralizati on of Special Elements in			urllib2 in Python 2.x through 2.7.17 and urllib		
Neutralizati on of Special Elements in			urllib2 in Python 2.x through 2.7.17 and urllib		
by a Downstrea m Component ('Injection')	-10-2019	4.3	in Python 3.x through 3.8.0. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the host component of a URL) followed by an HTTP header. This is similar to the CVE-2019-9740 query string issue and the CVE- 2019-9947 path string issue. (This is not exploitable when glibc has CVE-2016-10739 fixed.) CVE ID: CVE-2019- 18348	N/A	A-PYT-PYTH- 041119/644
CV Scoring Scale					

Weakness	Puk	olish Date	CVSS	Description & CVE ID			Pato	h	NCIIP	C ID	
QT											
qtbase											
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-1	10-2019	5	An out-of-bounds memory access in the generateDirectionalRuns() function in qtextengine.cpp in Qt qtbase 5.11.x and 5.12.x before 5.12.5 allows attackers to cause a denial of service by crashing an application via a text file containing many directional characters.				N/A		A-QT-Q' 041119	
				CVE ID : CVE-2019- 18281							
rambox											
rambox											
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	16-2	10-2019	8.5	There is a stored XSS in Rambox 0.6.9 that can lead to code execution. The XSS is in the name field while adding/editing a service. The problem occurs due to incorrect sanitization of the name field when being processed and stored. This allows a user to craft a payload for Node.js and Electron, such as an exec of OS commands within the onerror attribute of an IMG element. CVE ID: CVE-2019-17625				N/A		A-RAM- RAMB- 041119	/646
ratpack_project											
ratpack											
Improper		10-2019	5	An issue was discovered in		https://githu		A-RAT-RATP-			
CV Scoring Sca (CVSS)	ıle	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				Pato	:h	NCIIP	CID
Input Validation			to a m librar Defau is no w heade chara untru const with l Respo occur	nisuse of y class altHttpHovalidation of the cters. The steed date of the cters of	HTTP conus, if a is used FP headd HTTP itting car	ty there ntrol d to ers	b.com/ratpaceases/tar7.5, https://sb.com/ratpaceurity/ades/GHS/mvqp-q3wf9j	ck/rel g/v1. githu atpac ck/sec visori	041119	/647
rconfig			17513							
rconfig										
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	28-10-2019	10	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to ajaxServerSettingsChk.php because the rootUname parameter is passed to the exec function without filtering, which can lead to command execution. CVE ID: CVE-2019-16662				N/A		A-RCO-1 041119	
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	28-10-2019	9	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to search.crud.php because the catCommand parameter is passed to the exec function without filtering, which can lead to			N/A		A-RCO-1 041119		
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	D	escriptio	n & CVE ID)	Pato	h	NCIIF	PCID
			comn	nand exe	ecution.					
			CVE I	D : CVE	-2019-					
			1666	3						
repetier-serv	ver									
repetier-serv	ver									
Unrestricted Upload of File with Dangerous Type	25-10-2019	10	throu prope data s when print When with attack "exte config config remo After of the config on a s	Repetier-Server 0.8 through 0.91 does not properly validate the XML data structure provided when uploading a new printer configuration. When this is combined with CVE-2019-14450, an attacker can upload an "external command" configuration as a printer configuration, and achieve remote code execution. After exploitation, loading of the external command configuration is dependent on a system reboot or service restart. CVE ID: CVE-2019- 14451		KML ed d d d, an ieve ieve n. ding	https://repetier.server.co nowledg /security advisory	- om/k gebase y-	A-REP-1 041119	
reportlab					-2019-					
reportlab										
XML Injection (aka Blind XPath Injection)	16-10-2019	7.5	ReportLab through 3.5.26 allows remote code execution because of toColor(eval(arg)) in colors.py, as demonstrated by a crafted XML document with ' <span arbitrary="" by="" code.="" color="" cve="" cve-2019-<="" followed="" id:="" python="" td=""><td>N/A</td><td></td><td>A-REP-1 041119</td><td></td>			N/A		A-REP-1 041119		
			-						1	

(CVSS)

Weakness	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D		Pato	:h	NCIIP	C ID
				1762	6							
restaurant_n	nana	gement <u>.</u>	_system_	projec	t							
restaurant_n	nana	gement <u></u>	system									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-	10-2019	4.3	Resta System the "s screen CVE I	Sourcecodester Restaurant Management System 1.0 allows XSS via the "send a message" screen. CVE ID : CVE-2019- 18415				A		A-RES-REST- 041119/652	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-	10-2019	4.3	Sourcecodester Restaurant Management System 1.0 allows XSS via the Last Name field of a member. CVE ID: CVE-2019- 18416				N/	A		A-RES-I 041119	
rocket.chat												
rocket.chat												
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-	10-2019	4.3	allow ![title CVE I	Rocket.Chat before 2.1.0 allows XSS via a URL on a ![title] line. CVE ID : CVE-2019-17220		N/	A		A-ROC- 041119		
sagemath												
sagemathcel	l											
Improper Neutralizati on of Special Elements used in an OS Command	18-	10-2019	10	** DISPUTED ** An issue was discovered in SageMath Sage Cell Server through 2019-10-05. Python Code Injection can occur in the context of an internet facing web			N/A			A-SAG-SAGE- 041119/655		
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('OS			application. Malicious							
Command			actors can execute							
Injection')			arbitrary commands on							
			the underlying operating							
			system, as demonstrated							
			by an							
			import('os').popen('wh oami').read() line. NOTE:							
			the vendor's position is							
			that the product is							
			"vulnerable by design" and							
			the current behavior will							
			be retained.							
			CVE ID : CVE-2019-							
			17526							
schlix										
cms										
			** DISPUTED **							
			admin/app/mediamanage							
			r in Schlix CMS 2.1.8-7 allows Authenticated							
			Unrestricted File Upload,							
			leading to remote code							
			execution. NOTE: "While							
Unrestricted			inadvertently allowing a							
Upload of	04.40.0040	. .	PHP file to be uploaded via	27.74	A-SCH-CMS-					
File with	24-10-2019	6.5	Media Manager was an	N/A	041119/656					
Dangerous			oversight, it still requires		·					
Type			an admin permission. We							
			think it's pretty rare for an							
			administrator to exploit a							
			bug on his/her own site to own his/her own site."							
			CVE ID : CVE-2019-							
			11021							
semperplugins										
all_in_one_seo_pack										
Improper	16-10-2019	3.5	The all-in-one-seo-pack	N/A	A-SEM-ALL					
Neutralizati CV Scoring Sca			plugin before 3.2.7 for		11 001.1 1100_					
C) / C . C	via l									

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
on of Input During Web Page Generation ('Cross-site Scripting')			SEO F Store impro SEO-s for po plugin place	Press (a Pack) is s d XSS du oper enc specific c osts prov n via uns holder r D: CVE- 0	susceptil te to oding of descriptivided by safe eplacem	the f the ion the			041119	/657
sequelizejs										
sequelize										
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	29-10-2019	7.5	prior 5.8.11 SQL I path I prope MySQ	elize all v to 3.35.1 l are vul njection keys not erly esca L/Maria D: CVE- 8	1, 4.44.3 nerable due to J being ped for aDB dial	, and to SON the	N/A		A-SEQ-S 041119	_
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	29-10-2019	7.5	3.35.2 perfo due to not be saniti dialec	sequelize before version 3.35.1 allows attackers to perform a SQL Injection due to the JSON path keys not being properly sanitized in the Postgres dialect. CVE ID: CVE-2019- 10749			N/A		A-SEQ-S 041119	_
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL	17-10-2019	7.5	Sequelize, all versions prior to version 4.44.3 and 5.15.1, is vulnerable to SQL Injection due to sequelize.json() helper function not escaping values properly when formatting sub paths for JSON queries for MySQL,			https:// o/vuln/s JS- SEQUEL 459751,	SNYK-	A-SEQ-S 041119	-	
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

sitemagic sitemagic Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')			MariaDB and SQLite. CVE ID: CVE-2019- 10752 Sitemagic CMS 4.4.1 is affected by a Cross-Site-		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site			10752 Sitemagic CMS 4.4.1 is		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site			· ·		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site			· ·		
Neutralizati on of Input During Web Page Generation ('Cross-site			· ·		
	3-10-2019	4.3	Scripting (XSS) vulnerability, as it fails to validate user input. The affected components (index.php, upgrade.php) allow for JavaScript injection within both GET or POST requests, via a crafted URL or via the UpgradeMode POST parameter. CVE ID: CVE-2019- 18219	N/A	A-SIT-SITE- 041119/661
Cross-Site Request Forgery (CSRF)	3-10-2019	6.8	Sitemagic CMS 4.4.1 is affected by a Cross-Site-Request-Forgery (CSRF) issue as it doesn't implement any method to validate incoming requests, allowing the execution of critical functionalities via spoofed requests. This behavior could be abused by a remote unauthenticated attacker to trick Sitemagic users into performing unwarranted actions. CVE ID: CVE-2019-18220	N/A	A-SIT-SITE- 041119/662
slub_events_proj	nio at				

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	C ID	
slub_events										
Unrestricted Upload of File with Dangerous Type	16-10-2019	7.5	The slub_events (aka SLUB: Event Registration) extension through 3.0.2 for TYPO3 allows uploading of arbitrary files to the webserver. For versions 1.2.2 and below, this results in Remote Code Execution. In versions later than 1.2.2, this can result in Denial of Service, since the web space can be filled up with arbitrary files. CVE ID: CVE-2019-16700				https:// org/sec advisory 3-ext-sa 2019-02	urity/ y/typo -	A-SLU-S 041119	
Sonatype			1670	0						
nexus_iq_server										
Unrestricted Upload of File with Dangerous Type	21-10-2019	9	Repos before before code e	Sonatype Nexus Repository Manager 2.x before 2.14.15 and 3.x before 3.19, and IQ Server before 72, has remote code execution. CVE ID: CVE-2019- 16530				suppo ype.co n- les/3 32453	A-SON-1 041119	
nexus_repos	itory_manage	r								
Improper Privilege Managemen t	16-10-2019	6.5	Repos before Remo	Sonatype Nexus Repository Manager 2.x before 2.14.15 allows Remote Code Execution. CVE ID: CVE-2019- 15893			https://suppo rt.sonatype.co m/hc/en- us/articles/3 60035055794		A-SON-NEXT 041119/66	
Unrestricted Upload of File with Dangerous	21-10-2019	9	Sonatype Nexus Repository Manager 2.x before 2.14.15 and 3.x before 3.19, and IQ Server			ζ	https://suppo rt.sonatype.co m/hc/en- us/articles/3		A-SON-NEXU- 041119/666	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
Type			code	e 72, has executio D : CVE- 0	n.		6003613	32453		
sourcecodest	ter									
restaurant_n	nanagement_s	ystem								
Cross-Site Request Forgery (CSRF)	24-10-2019	6.8	Resta Syste an ad Cross vulne of CSI could tricki into e code entry page.	D : CVE-	anagemonaffected affected.puest Founder to a ction. The contraction artical desired arbitra g a staffufted HT	by hp rgery lack his ker rator	N/A		A-SOU-I 041119	
Unrestricted Upload of File with Dangerous Type	24-10-2019	6.5	Sourcecodester Restaurant Management System 1.0 allows an authenticated attacker to upload arbitrary files that can result in code execution. The issue occurs because the application fails to adequately sanitize user- supplied input, e.g., "add a new food" allows .php files. CVE ID: CVE-2019- 18417			N/A		A-SOU-I 041119		
online_gradi		(0					NI / A			
Cross-Site	23-10-2019	6.8	Sourc	cecodest	er Onlin	e 	N/A		A-SOU-0	ONLI-
CV Scoring Sca (CVSS)	ole 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		
Request Forgery (CSRF)			Grading System 1.0 is affected by a Cross Site Request Forgery vulnerability due to a lack of CSRF protection. This could lead to an attacker tricking the administrator into executing arbitrary code via a crafted HTML page, as demonstrated by a Create User action at the admin/modules/user/con troller.php?action=add URI. CVE ID: CVE-2019-18280		041119/669		
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	23-10-2019	7.5	Sourcecodester Online Grading System 1.0 is vulnerable to unauthenticated SQL injection and can allow remote attackers to execute arbitrary SQL commands via the student, instructor, department, room, class, or user page (id or classid parameter). CVE ID: CVE-2019- 18344	N/A	A-SOU-ONLI- 041119/670		
sr_freecap_p	roject						
sr_freecap							
Improper Input Validation	16-10-2019	7.5	The sr_freecap (aka freeCap CAPTCHA) extension 2.4.5 and below and 2.5.2 and below for TYPO3 fails to sanitize user input, which allows execution of arbitrary Extbase actions, resulting	https://typo3. org/security/ advisory/typo 3-ext-sa- 2019-018/	A-SRSR_F- 041119/671		
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				
			in Remote Code Execution. CVE ID: CVE-2019- 16699						
sudo_project									
sudo									
Improper Input Validation	17-10-2019	9	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#\$((0xffffffff))" command. CVE ID: CVE-2019-14287	https://securi ty.netapp.com /advisory/nta p-20191017- 0003/, https://suppo rt.f5.com/csp /article/K537 46212?utm_s ource=f5supp ort&utm _medium=RSS , https://www. sudo.ws/alert s/minus_1_ui d.html	A-SUD-SUDO- 041119/672				
Symantec									
messaging_g	ateway				,				
Information Exposure	24-10-2019	2.7	Symantec Messaging Gateway (prior to 10.7.0), may be susceptible to an information disclosure issue, which is a type of vulnerability that could potentially allow unauthorized access to data. CVE ID: CVE-2019-9699	https://suppo rt.symantec.c om/en_US/art icle.SYMSA14 82.html	A-SYM-MESS- 041119/673				
Teamviewer									
teamviewer									
Untrusted	24-10-2019	6.9	A DLL side loading	https://comm	A-TEA-TEAM-				
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
Search Path			vulnerability in the Windows Service in TeamViewer versions up to 11.0.133222 (fixed in 11.0.214397), 12.0.181268 (fixed in 12.0.214399), 13.2.36215 (fixed in 13.2.36216), and 14.6.4835 (fixed in 14.7.1965) on Windows could allow an attacker to perform code execution on a target system via a service restart where the DLL was previously installed with administrative privileges. Exploitation requires that an attacker be able to create a new file in the TeamViewer application directory; directory permissions restrict that by default. CVE ID: CVE-2019- 18196	unity.teamvie wer.com/t5/A nnouncement s/Security- bulletin-CVE- 2019- 18196/td- p/74564	041119/674
Tenable					
nessus					
Improper Input Validation	23-10-2019	4	Nessus versions 8.6.0 and earlier were found to contain a Denial of Service vulnerability due to improper validation of specific imported scan types. An authenticated, remote attacker could potentially exploit this vulnerability to cause a Nessus scanner to become temporarily unresponsive.	N/A	A-TEN-NESS- 041119/675
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
			CVE ID : CVE-2019-3982		
theia_xml_ex	tension_projec	ct			
theia_xml_ex	tension				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	4	in XML Language Service.java in XML Language Server (aka lsp4xml) before 0.9.1, as used in Red Hat XML Language Support (aka vscode-xml) before 0.9.1 for Visual Studio and other products, allows a remote attacker to write to arbitrary files via Directory Traversal. CVE ID: CVE-2019-	https://githu b.com/angelo zerr/lsp4xml/ blob/master/ CHANGELOG. md#others	A-THE-THEI- 041119/676
			18212		
XML Injection (aka Blind XPath Injection)	23-10-2019	6.5	XML Language Server (aka lsp4xml) before 0.9.1, as used in Red Hat XML Language Support (aka vscode-xml) before 0.9.1 for Visual Studio and other products, allows XXE via a crafted XML document, with resultant SSRF (as well as SMB connection initiation that can lead to NetNTLM challenge/response capture for password cracking). This occurs in extensions/contentmodel/participants/diagnostics/L SPXMLParserConfiguratio n.java. CVE ID: CVE-2019-19213	https://githu b.com/angelo zerr/lsp4xml/ blob/master/ CHANGELOG. md#others	A-THE-THEI- 041119/677
th own a alti-			18213		
themooltipas	SS				

Weakness	Pul	blish Date	e CVSS	D	escriptio	n & CVE I	D		Pato	h	NCIIF	PC ID
moolticute												
Cleartext Transmissio n of Sensitive Information	22-	10-2019	4.3	Moold (and version Acces	ticute the possibly ons) has control of the control	rough 0. earlier Incorre		N	N/A		A-THE- 041119	
Thycotic								<u> </u>				
secret_serve	r											
Server-Side Request Forgery (SSRF)	23-	10-2019	7.5	disco Web Secre	RF issue vered in launcher t Server D : CVE	the lega in Thyo before 2	cotic	N/A			/A A-THY-SE 041119/6	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-	10-2019	4.3	disco Secre (issue	SS issue vered in t Server e 1 of 2). (D: CVE	Thycoti before		N	N/A		A-THY-SECR- 041119/680	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-	10-2019	4.3	disco Secre (issue	SS issue vered in t Server e 2 of 2). TD: CVE	Thycoti before		N/A			A-THY- 041119	
Tightvnc												
tightvnc												
Out-of- bounds Write	29-	10-2019	7.5	TightVNC code version 1.3.10 contains heap buffer overflow in rfbServerCutText handler,			N/A		A-TIG-TIGH- 041119/682			
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	Pul	olish Date	CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
				result This a explo conne CVE I	which can potentially result code execution This attack appear to be exploitable via network connectivity. CVE ID: CVE-2019-15678 TightVNC code version						
Out-of- bounds Write	29-	10-2019	7.5	1.3.10 buffer Initial function potential execution appears via necessity.	ocontair coverflo liseRFB(ion, which itially re tion. The ar to be e etwork c	ns heap w in Connecti ch can sult code is attack exploital onnectiv	on e :	N/A		A-TIG-T 041119	
NULL Pointer Dereference	29-	10-2019	5	1.3.10 point. Hand: which System appears via ne	TightVNC code version 1.3.10 contains null pointer dereference in HandleZlibBPP function, which results Denial of System (DoS). This attack appear to be exploitable via network connectivity. CVE ID: CVE-2019-			N/A		A-TIG-T 041119	
tomedo											
server											
Insufficientl y Protected Credentials	18-	10-2019	5	Serve comm Vendo HTTP can be unaut authe	The Customer's Tomedo Server in Version 1.7.3 communicates to the Vendor Tomedo Server via HTTP (in cleartext) that can be sniffed by unauthorized actors. Basic authentication is used for the authentication, making			N/A		A-TOM- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
topmeeting			it possible to base64 decode the sniffed credentials and discover the username and password. CVE ID: CVE-2019- 17393							
topmeeting										
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	17-10-2019	5	vulned discomplished discompli	injection rability vered in e version of the versio	was TOPMe 1 8.8). An 1 se a uni 1 query 1 a search 1 feature 1 schema 1 ssword.	on n e to and	https://cert.org.iwanvn/2019070https://twcert.o/en/cp-3019-f002.html	tw/ta TVN- 001, www. rg.tw 128-	A-TOP-7 041119	
Information Exposure	17-10-2019	5	version show and propage attack sension brow of the CVE I	TOPMeeting before version 8.8 (2019/08/19) shows attendees account and password in front end page that allows an attacker to obtain sensitive information by browsing the source code of the page. CVE ID: CVE-2019-13410			https://cert.org.iwanvn/2019070https://twcert.o/en/cp-3020-272.html	tw/ta TVN- 002, www. rg.tw 128-	A-TOP-7 041119	
totemo			•							
totemodata			1							
Improper Neutralizati on of Input	22-10-2019	3.5	totemodata 3.0.0_b936 has XSS via a folder name. CVE ID: CVE-2019-			N/A		A-TOT-7 041119		
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	D	escriptio	n & CVE I	D		Pato	h	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')			17189								
Trendmicro deep_securit	v										
Information Exposure	17-10-2019	4.3	Mana (Vers 12.0) a cert trans comm text. 7 confid does or ava	Deep Sec ger applions 10. when can way mit inition can way dentiality dentiality dentiality D: CVE	lication 0, 11.0 a onfigure , may al LDAP on in cle v result i y impac act integ	ed in ar n t but	N/	/A		A-TRE-1 041119	
Improper Input Validation	17-10-2019	6.6	Versions 10.0, 11.0 and 12.0 of the Trend Micro Deep Security Agent are vulnerable to an arbitrary file delete attack, which may lead to availability impact. Local OS access is required. Please note that only Windows agents are affected. CVE ID: CVE-2019-15627		N/	/A		A-TRE-1			
anti-threat_t	oolkit										
Improper Input Validation	21-10-2019	5.1	Trend Micro Anti-Threat Toolkit (ATTK) versions 1.62.0.1218 and below have a vulnerability that may allow an attacker to place malicious files in the			N,	/A		A-TRE-2 041119		
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	Descriptio	n & CVE II		Pato	h	NCIIP	C ID
			same director leading to ark remote code (RCE) when e	oitrary execution	n				
			CVE ID : CVE	-2019-9	491				
typestack_cla	ass-validator_p	roject							
typestack_cla	ass-validator								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	7.5	In TypeStack validator 0.10 input validation bypassed becommer internal attributes overwritten was conflicting not though there forbidUnknown parameter the used to reduce this bypass, the not documen most develop input validation vulnerable demanner. With vulnerability, can launch SO or XSS attacks arbitrary male NOTE: a softwaintainer against in not documen finding but sumuch of the refor the risk lied different process.	D.2, validation can be ause certo butes can be is an option ted and to be attacker a	e tain h be h dional sek of n is shus gure e secondary.	N/A		A-TYP-7 041119	
	fice_converter_	projec	et						
	fice_converter								
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
Server-Side Request Forgery (SSRF)	21-10-2019	5	The unoconv package before 0.9 mishandles untrusted pathnames, leading to SSRF and local file inclusion. CVE ID: CVE-2019-	N/A	A-UNI-UNIV- 041119/693
url_redirect_	nroject		17400		
url_redirect_	project				
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	16-10-2019	7.5	The url_redirect (aka URL redirect) extension through 1.2.1 for TYPO3 fails to properly sanitize user input and is susceptible to SQL Injection. CVE ID: CVE-2019-16682	https://typo3. org/security/ advisory/typo 3-ext-sa- 2019-015/	A-URL-URL 041119/694
verodin					
director					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	3.5	There is Stored XSS in Verodin Director 3.5.3.0 and earlier via input fields of certain tooltips, and on the Tags, Sequences, and Actors pages. CVE ID: CVE-2019- 10715	N/A	A-VER-DIRE- 041119/695
Insufficientl y Protected Credentials	21-10-2019	4	An Information Disclosure issue in Verodin Director 3.5.3.1 and earlier reveals usernames and passwords of integrated security technologies via a /integrations.json JSON REST API request. CVE ID: CVE-2019-	N/A	A-VER-DIRE- 041119/696

Weakness	Pul	olish Date	cvss	D	escriptio	1 & CVE I	D	Pat	ch	NCIIP	CID
				1071	6						
video_conver	ter_	project									
video_conver	ter										
Missing Release of Resource after Effective Lifetime	19-	10-2019	6.8	The Video_Converter app 0.1.0 for Nextcloud allows denial of service (CPU and memory consumption) via multiple concurrent conversions because many FFmpeg processes may be running at once. (The workload is not queued for serial execution.) CVE ID: CVE-2019-18214			N/A		A-VID-V 041119		
Videolan											
vlc_media_pl	ayer										
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-	10-2019	4.6	VLC m with l Data t Addro Flow libqt_ nse_: 03b9	When executing VideoLAN VLC media player 3.0.8 with libqt on Windows, Data from a Faulting Address controls Code Flow starting at libqt_plugin!vlc_entry_lice nse_3_0_0f+0x000000000 03b9aba. CVE ID: CVE-2019-			N/A		A-VID-V 041119	_
Vmware											
cloud_founda	tion										
Incorrect Default Permissions	18-	10-2019	5	Access vulne vulne proje use the create	Harbor API has a Broken Access Control vulnerability. The vulnerability allows project administrators to use the Harbor API to create a robot account with unauthorized push			http://v mware.o ecurity/ ories/V 2019- 0016.ht	com/s 'advis MSA-	A-VMW CLOU- 041119	
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	D	escription	n & CVE II	D	Pate	:h	NCIIP	C ID	
			and/or pull access permissions to a project they don't have access or control for. The Harbor API did not enforce the proper project permissions and project scope on the API request to create a new robot account. CVE ID : CVE-2019- 16919 Harbor API has a Broken								
harbor_conta	iner_registry										
Incorrect Default Permissions	18-10-2019	5	Access vulne vulne proje use the create with and/o perm they contrade proper perm scope to create accounts.	and/or pull access permissions to a project they don't have access or control for. The Harbor API did not enforce the proper project permissions and project scope on the API request to create a new robot account. CVE ID : CVE-2019-		http://v mware.o ecurity/ ories/VI 2019- 0016.htm	com/s advis MSA-	A-VMW HARB- 041119			
wacom driver											
Improper Privilege Managemen t	24-10-2019	7.2	escala exists	An exploitable privilege escalation vulnerability exists in the Wacom, driver version 6.3.32-3,			N/A		A-WAC-DRIV- 041119/701		
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
			update helper service in the startProcess command. The command takes a user-supplied script argument and executes it under root context. A user with local access can use this vulnerability to raise their privileges to root. An attacker would need local access to the machine for a successful exploit. CVE ID: CVE-2019-5012		
Improper Privilege Managemen t	24-10-2019	7.2	An exploitable privilege escalation vulnerability exists in the Wacom, driver version 6.3.32-3, update helper service in the start/stopLaunchDProcess command. The command takes a user-supplied string argument and executes launchctl under root context. A user with local access can use this vulnerability to raise load arbitrary launchD agents. An attacker would need local access to the machine for a successful exploit. CVE ID: CVE-2019-5013	N/A	A-WAC-DRIV- 041119/702
whatsapp					
whatsapp					
Improper Restriction of Operations	23-10-2019	7.5	A heap buffer overflow bug in libpl_droidsonroids_gif before 1.2.19, as used in	https://www. facebook.com /security/adv isories/cve-	A-WHA- WHAT- 041119/703
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
within the Bounds of a Memory Buffer			WhatsApp for Android before version 2.19.291 could allow remote attackers to execute arbitrary code or cause a denial of service. CVE ID: CVE-2019-11933				2019-11	933		
Wikidsystem	IS									
2fa_enterpris	se_server									
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	17-10-2019	6.5	vulne proce 2FA F throu allow user t SQL c proce paran		in sp in Wil se Serve -b2053 henticat te arbitr ds via th	r ed ary	N/A		A-WIK-: 041119	_
Cross-Site Request Forgery (CSRF)	17-10-2019	6.8	A CSRF issue in WiKID 2FA Enterprise Server through 4.2.0-b2053 allows a remote attacker to trick an authenticated user into performing unintended actions such as (1) create or delete admin users; (2) create or delete groups; or (3) create, delete, enable, or disable normal users or devices. CVE ID: CVE-2019- 17118				N/A		A-WIK-2 041119	_
two_factor_a	uthentication _.	enterp	orise_s	erver						
Improper	17-10-2019	6.5	WiKI	D Enterp	rise 2F	A	N/A		A-WIK-	ΓW0
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	Pul	blish Date	е	CVSS	D	Description & CVE ID				Patc	h	NCIIP	CID
Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')					Serve b204 inject searc endp doma used, query build funct CVE I	authentication) Enterprise Server through 4.2.0- b2047 is vulnerable to SQL injection through the searchDevices.jsp endpoint. The uid and domain parameters are used, unsanitized, in a SQL query constructed in the buildSearchWhereClause function. CVE ID: CVE-2019- 16917						041119	/706
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-	10-2019	Ð	4.3	cross vulne 2FA I throu allow inject or HT /WiK istrat preRe parar reflect script imme file is malic and c when Regis is use	A stored and reflected cross-site scripting (XSS) vulnerability in WiKID 2FA Enterprise Server through 4.2.0-b2047 allows remote attackers to inject arbitrary web script or HTML via /WiKIDAdmin/userPrereg istration.jsp. The preRegistrationData parameter is vulnerable: a reflected cross-site scripting occurs immediately after a .csv file is uploaded. The malicious script is stored and can be executed again when the List Pre-Registration functionality is used. CVE ID: CVE-2019-				I/A		A-WIK-' 041119	
Improper Neutralizati on of Input	17-	10-2019	9	4.3	Multiple cross-site scripting (XSS) vulnerabilities in WiKID				N	I/A		A-WIK-' 041119	_
CV Scoring Sca (CVSS)	ile	0-1	:	1-2	2-3	3-4	4-5	5-6		6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web			2FA Enterprise Server		
Page			through 4.2.0-b2047 allow		
Generation			remote attackers to inject		
('Cross-site			arbitrary web script or		
Scripting')			HTML that is triggered		
			when Logs.jsp is visited.		
			The rendered_message		
			column is retrieved and		
			displayed, unsanitized, on		
			Logs.jsp. A remote attack		
			can populate the		
			rendered_message column		
			with malicious values via:		
			(1) H parameter to		
			/wikid/servlet/com.wikid		
			systems.server.GetDomain		
			Hash (2) S parameter to: -		
			/wikid/DomainData -		
			/wikid/PreRegisterLooku		
			p - /wikid/PreRegister -		
			/wikid/InitDevice -		
			/wikid/servlet/InitDevice		
			2S -		
			/wikid/servlet/InitDevice		
			3S -		
			/servlet/com.wikidsystem		
			s.server.InitDevice2S -		
			/servlet/com.wikidsystem		
			s.server.InitDevice3S -		
			/servlet/com.wikidsystem		
			s.server.InitDevice4S -		
			/wikid/servlet/com.wikid		
			systems.server.InitDevice		
			· · · · · · · · · · · · · · · · · · ·		
			4AES - /wikid/servlet/com.wikid systems.server.InitDevice 5AES (3) a parameter to: - /wikid/PreRegisterLooku p - /wikid/InitDevice - /wikid/servlet/InitDevice 2S -		

CV Scoring Scale	0-1	1_2	2-3	3_/1	1-5	5-6	6-7	7-8	8_Q	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	De	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
			3S - /servl s.serv /servl s.serv /servl s.serv /wikid syster 4AES /wikid syster 5AES. CVE II	d/servle ns.serve D : CVE -	wikidsy evice2S wikidsy evice3S wikidsy evice4S et/com.v er.InitDe	vstem - vstem - vstem - vstem - wikid evice				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	4.3	A stored and reflected cross-site scripting (XSS) vulnerability in WiKID 2FA Enterprise Server through 4.2.0-b2047 allow remote attackers to inject arbitrary web script or HTML via /WiKIDAdmin/groups.jsp. The groupName parameter is vulnerable: the reflected cross-site scripting occurs immediately after the group is created. The malicious script is stored and will be executed again whenever /WiKIDAdmin/groups.jsp is visited. CVE ID: CVE-2019-			N/A		A-WIK-' 041119		
Improper Neutralizati	17-10-2019	6.5	Multiple SQL injection vulnerabilities in Logs.jsp			N/A		A-WIK- 041119		
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	NCIIPC ID
on of Special Elements used in an SQL Command ('SQL Injection')			in WiKID 2FA Enterprise Server through 4.2.0- b2053 allow authenticated users to execute arbitrary SQL commands via the source or subString parameter. CVE ID: CVE-2019- 17119		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	4.3	A stored and reflected cross-site scripting (XSS) vulnerability in WiKID 2FA Enterprise Server through 4.2.0-b2047 allow remote attackers to inject arbitrary web script or HTML via /WiKIDAdmin/adm_usrs.j sp. The usr parameter is vulnerable: the reflected cross-site scripting occurs immediately after the user is created. The malicious script is stored and will be executed whenever /WiKIDAdmin/adm_usrs.j sp is visited. CVE ID: CVE-2019-17120	N/A	A-WIK-TWO 041119/711
Wordpress					
wordpress					
Server-Side Request Forgery (SSRF)	17-10-2019	7.5	WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because URL validation does not consider the interpretation of a name as a series of hex	N/A	A-WOR- WORD- 041119/712
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
			characters. CVE ID : CVE-2019- 17669		
Server-Side Request Forgery (SSRF)	17-10-2019	7.5	WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because Windows paths are mishandled during certain validation of relative URLs. CVE ID: CVE-2019- 17670	N/A	A-WOR- WORD- 041119/713
Information Exposure	17-10-2019	5	In WordPress before 5.2.4, unauthenticated viewing of certain content is possible because the static query property is mishandled. CVE ID: CVE-2019-17671	N/A	A-WOR- WORD- 041119/714
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	4.3	WordPress before 5.2.4 is vulnerable to a stored XSS attack to inject JavaScript into STYLE elements. CVE ID: CVE-2019-17672	N/A	A-WOR- WORD- 041119/715
Improper Input Validation	17-10-2019	5	WordPress before 5.2.4 is vulnerable to poisoning of the cache of JSON GET requests because certain requests lack a Vary: Origin header. CVE ID: CVE-2019-17673	N/A	A-WOR- WORD- 041119/716
Improper Neutralizati	17-10-2019	3.5	WordPress before 5.2.4 is vulnerable to stored XSS	N/A	A-WOR- WORD-

3-4

2-3

1-2

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Pato	h	NCIIPC	ID
on of Input During Web Page Generation			(cross-site scripting) via the Customizer. CVE ID : CVE-2019- 17674			041119/	717
('Cross-site Scripting')							
Cross-Site Request Forgery (CSRF)	17-10-2019	6.8	WordPress before 5.2.4 does not properly consider type confusion during validation of the referer in the admin pages, possibly leading to CSRF.	N/A		A-WOR- WORD- 041119/	718
			CVE ID : CVE-2019- 17675				
wp-events-p	lugin						
events_mana	iger						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	The events-manager plugin through 5.9.5 for WordPress (aka Events Manager) is susceptible to Stored XSS due to improper encoding and insertion of data provided to the attribute map_style of shortcodes (locations_map and events_map) provided by the plugin. CVE ID: CVE-2019-16523	N/A		A-WPE' 041119/	-
X							
x_server							
Out-of- bounds Write	16-10-2019	4.6	In X.Org X Server 1.20.4, there is a stack-based buffer overflow in the function XQueryKeymap. For example, by sending ct.c_char 1000 times, an	N/A		A-X-X_SE 041119/	
CV Scoring Sca (CVSS)	o-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 can cause a denial of service (application crash) or possibly have unspecified other impact. CVE ID: CVE-2019-17624		
xml_languag	 e_server_proje	ct	1.021		
xml_server_p	project				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	4	in XML Language Server (aka lsp4xml) before 0.9.1, as used in Red Hat XML Language Support (aka vscode-xml) before 0.9.1 for Visual Studio and other products, allows a remote attacker to write to arbitrary files via Directory Traversal. CVE ID: CVE-2019- 18212	https://githu b.com/angelo zerr/lsp4xml/ blob/master/ CHANGELOG. md#others	A-XML-XML 041119/721
XML Injection (aka Blind XPath Injection)	23-10-2019	6.5	XML Language Server (aka lsp4xml) before 0.9.1, as used in Red Hat XML Language Support (aka vscode-xml) before 0.9.1 for Visual Studio and other products, allows XXE via a crafted XML document, with resultant SSRF (as well as SMB connection initiation that can lead to NetNTLM challenge/response capture for password cracking). This occurs in extensions/contentmodel/participants/diagnostics/L SPXMLParserConfiguratio	https://githu b.com/angelo zerr/lsp4xml/ blob/master/ CHANGELOG. md#others	A-XML-XML 041119/722

CV Scoring Scale	0-1	1_2	2-3	2-1	1-5	5-6	6-7	7_8	8 _0	0-10
(CVSS)	0-1	1-2	2-3	3-4	4-3	3-0	0-7	7-8	0-3	9-10

Weakness	Puk	olish Date	cvss	D	escriptio	n & CVE II	D	Pa	tch	NCIIP	PC ID
				n.java CVE I 1821	D : CVE-	2019-					
Xmlsoft				_							
libxslt											
Use After Free	18-1	10-2019	6.8	transf 1.1.33 isn't r circum releva happe reuse bound and m buffer or un be dis	bounds check could fail and memory outside a buffer could be written to, or uninitialized data could be disclosed. CVE ID: CVE-2019-		N/A		A-XML- 041119		
xnat	<u> </u>										
xnat											
Improper Restriction of XML External Entity Reference ('XXE')	23-1	10-2019	4	allow POST	TL XNAT s XXE at request D : CVE-	tacks via body.	a a	N/A		A-XNA- 041119	
yalehome				•							
yale_bluetoo	th_ke	ey									
Improper Authenticati on	16-3	10-2019	3.3	The Yale Bluetooth Key application for mobile devices allows unauthorized unlock actions by sniffing Bluetooth Low Energy (BLE) traffic during one			N/A		A-YAL-Y 041119		
CV Scoring Sca (CVSS)	ile	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
			authorized unlock action, and then calculating the authentication key via simple computations on the hex digits of a valid authentication request. This affects the Yale ZEN-R lock and unspecified other locks.		
			CVE ID : CVE-2019- 17627		
youphptube					
youphptube					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	25-10-2019	6.5	An exploitable SQL injection vulnerability exists in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and,in certain configuration, access the underlying operating system. CVE ID: CVE-2019-5114	N/A	A-YOU-YOUP- 041119/726
Improper Neutralizati on of Special Elements used in an SQL Command	25-10-2019	6.5	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause a SQL injection. An attacker can	N/A	A-YOU-YOUP- 041119/727

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system. CVE ID: CVE-2019-5116		
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	25-10-2019	6.5	Exploitable SQL injection vulnerabilities exists in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system. CVE ID: CVE-2019-5117	N/A	A-YOU-YOUP- 041119/728
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	25-10-2019	6.5	An exploitable SQL injection vulnerability exist in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing	N/A	A-YOU-YOUP- 041119/729
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				P	atch	NCIIF	CID
			SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system. CVE ID: CVE-2019-5119							
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	25-10-2019	6.5	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system. CVE ID: CVE-2019-5120			N/A		A-Y0U-Y0UP- 041119/730		
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	25-10-2019	6.5	SQL injection vulnerabilities exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter uuid in /objects/pluginSwitch.jso n.php			N/A		A-YOU-YOUP- 041119/731		
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	Publish Date CVSS Description & CVE ID		Patch	NCIIPC ID	
			CVE ID : CVE-2019-5121			
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	25-10-2019	6.5	SQL injection vulnerabilities exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter name in /objects/pluginSwitch.jso n.php. CVE ID: CVE-2019-5122	N/A	A-YOU-YOUP- 041119/732	
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	25-10-2019	6.5	Specially crafted web requests can cause SQL injections in YouPHPTube 7.6. An attacker can send a web request with Parameter dir in /objects/pluginSwitch.jso n.php. CVE ID: CVE-2019-5123	N/A	A-YOU-YOUP- 041119/733	
youphptube_	encoder					
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	25-10-2019	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Url in /objects/getImage.php is vulnerable to a command		N/A	A-YOU-YOUP- 041119/734	

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID			Pato	h	NCIIP	CID
			injection att		127				
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	25-10-2019	7.5	A command been found YouPHPTub successful a allow an att compromise Exploitable unauthentic injections ex YouPHPTub a plugin for encoder fun YouPHPTub parameter by objects/gep is vulnerate command in CVE ID: CV	N/A		A-YOU- 041119			
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	25-10-2019	7.5	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Url in /objects/getSpiritsFromVi deo.php is vulnerable to a command injection attack. CVE ID: CVE-2019-5129		N/A		A-Y0U- 041119		
zenspider			3.212.07						
•									
CV Scoring Sca	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
ruby_parser-	legacy		L		
Incorrect Permission Assignment for Critical Resource	24-10-2019	4.6	The ruby_parser-legacy (aka legacy) gem 1.0.0 for Ruby allows local privilege escalation because of world-writable files. For example, if the brakeman gem (which has a legacy dependency) 4.5.0 through 4.7.0 is used, a local user can insert malicious code into the ruby_parser-legacy-1.0.0/lib/ruby_parser/leg acy/ruby_parser.rb file.	N/A	A-ZEN-RUBY- 041119/737
			CVE ID : CVE-2019- 18409		
			Operating System		
Apple					
mac_os					
Improper Privilege Managemen t	24-10-2019	7.2	An exploitable privilege escalation vulnerability exists in the Wacom, driver version 6.3.32-3, update helper service in the startProcess command. The command takes a user-supplied script argument and executes it under root context. A user with local access can use this vulnerability to raise their privileges to root. An attacker would need local access to the machine for a successful exploit. CVE ID: CVE-2019-5012	N/A	O-APP-MAC 041119/738

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pate	:h	NCIIP	C ID
Improper Privilege Managemen t	24-10-2019	7.2	An exploitable privilege escalation vulnerability exists in the Wacom, driver version 6.3.32-3, update helper service in the start/stopLaunchDProcess command. The command takes a user-supplied string argument and executes launchctl under root context. A user with local access can use this vulnerability to raise load arbitrary launchD agents. An attacker would need local access to the machine for a successful exploit. CVE ID: CVE-2019-5013			N/A		O-APP-1 041119	_	
Incorrect Type Conversion or Cast	17-10-2019	7.5	version and e 2015 and e 2015 earlie confu Succession and e 2015 could	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.		https:// adobe.co curity/p ts/acrob sb19-49	om/se roduc oat/ap	O-APP-1 041119	_	
Concurrent Execution using Shared Resource with	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier,			https://adobe.co curity/p ts/acrob sb19-49	om/se roduc oat/ap	O-APP-1 041119	_	
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
Improper Synchroniza tion ('Race Condition')			2015.006.30503 and earlier, and 2015.006.30503 and earlier have a race condition vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8162		
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8163	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/742
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8164	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/743

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8165	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/744
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a buffer overrun vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/745
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/746
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
			confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8167		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8168	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/747
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8169	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/748
Improper Restriction of Operations	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap	O-APP-MAC 041119/749

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Pub	lish Date	cvss	Description & CVE ID			D	Pato	h	NCIIP	C ID
within the Bounds of a Memory Buffer				and e 2015 earlie 2015 earlie overf Succe could code	earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8170				html		
Out-of- bounds Write	17-1	0-2019	6.8	version and explored arbits	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.			https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_
Out-of- bounds Read	17-1	0-2019	4.3	version and example and example and example 2015 example boun Succession could	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			https://l adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_
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	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
				CVE I	D : CVE	2019-8	172				
Out-of- bounds Read	17-	10-2019	4.3	version and e 2017, earlie 2015, earlie bound Succe could disclo	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8173 Adobe Acrobat and Reader				helpx. om/se roduc at/ap .html	0-APP-1 041119	
NULL Pointer Dereference	17-	10-2019	6.8	version and e 2017, earlie and e 2015, earlie point vulne explo				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	0-APP-1 041119	_
Use After Free	17-	10-2019	6.8	version and e 2017 earlier and e 2015 earlier	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_
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
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8175		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8176	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/755
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8177	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/756
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,	https://helpx. adobe.com/se curity/produc	O-APP-MAC 041119/757

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8178	ts/acrobat/ap sb19-49.html	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8179	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/758
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/759
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
			code execution .		
			CVE ID : CVE-2019-8180		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/760
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8182	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/761
Improper Restriction of Operations within the Bounds of a Memory	17-10-2019	9.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/762

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Buffer			earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8183		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8184	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/763
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8185	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/764
Out-of-	17-10-2019	10	Adobe Acrobat and Reader	https://helpx.	O-APP-MAC
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	
bounds Write			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of- bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8186	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/765	
Use After Free	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8187	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/766	
Use After Free	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/767	
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	NCIIPC ID	
			Successful exploitation could lead to arbitrary code execution .			
			CVE ID : CVE-2019-8188			
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8189	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/768	
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8190	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/769	
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/770	
Write CV Scoring Sc (CVSS)	ale 0-1	1-2			8-9 9-	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of- bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8191		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8192	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/771
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/772

Weakness	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
				CVE I	D : CVE	2019-8	193				
Out-of- bounds Read	17-	10-2019	5	version and e 2017, earlie 2015, earlie bound Succe could disclo	ons, 201 arlier, 011.301 ar, 2017. arlier, 006.305 ar, and 006.305 ar have a ds read v assful ex lead to osure.	011.301 503 and	48 classification	https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	0-APP-1 041119	_
NULL Pointer Dereference	17-	10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and			https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_	
NULL Pointer Dereference	17-	10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and			https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html			/se duc /ap	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			point vulne explo arbiti	er have a er dereferability. itation cary code D: CVE-	erence Success ould lea e executi	ful d to ion .				
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	7.5	2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8197				https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_
Out-of- bounds Read	17-10-2019	5	2015.006.30503 and earlier, and 2015.006.30503 and			https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_	
Out-of- bounds Write	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,				https://helpx. adobe.com/se curity/produc		O-APP-MAC 041119/778	
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
			2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8199	ts/acrobat/ap sb19-49.html	
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8200	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/779
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/780
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
			disclosure.		
			CVE ID : CVE-2019-8201		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8202 Adobe Acrobat and Reader		O-APP-MAC 041119/781
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8203	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/782
Out-of- bounds Read	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/783

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have an out-of- bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8204		
NULL Pointer Dereference	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/784
Out-of- bounds Write	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8206	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/785
Out-of-	17-10-2019	5	Adobe Acrobat and Reader	https://helpx.	O-APP-MAC
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	NCIIPC ID
bounds Read			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8207	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/786
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8208	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/787
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	0-APP-MAC 041119/788
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
			Successful exploitation could lead to arbitrary code execution.		
			CVE ID : CVE-2019-8209		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8210	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	0-APP-MAC 041119/789
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8211	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/790
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/791
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	NCIIPC ID
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8212		
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8213	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/792
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/793

Weakness	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID						
				CVE I	D : CVE	-2019-8	214										
Use After Free	17-	10-2019	7.5	version and experience with the control of the cont	ons, 201 arlier, .011.301 er, 2017. arlier, .006.305 er, and .006.305 er have a rulnerab essful ex lead to execution	011.301 503 and 503 and in use af ility. ploitatio	0040 48 ter on	https://badobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	0-APP-1 041119	_						
Out-of- bounds Read	17-	10-2019	5	version and e 2017 earlie 2015 earlie boun Succes could discle	2015.006.30503 and earlier, and 2015.006.30503 and			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_						
Use After Free	17-	10-2019	6.8	version and e 2017 earlie and e 2015 earlie	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and			versions , 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and		versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and		versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and		https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html		O-APP-N 041119	_
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
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8217		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8218	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/797
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8219	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/798
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,	https://helpx. adobe.com/se curity/produc	O-APP-MAC 041119/799

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8220	ts/acrobat/ap sb19-49.html	
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8221	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/800
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/801
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
			disclosure.		
			CVE ID : CVE-2019-8222		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/802
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8224	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/803
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/804

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.		
			CVE ID : CVE-2019-8225		
Information Exposure	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an incomplete implementation of security mechanism vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-APP-MAC 041119/805
Improper Privilege Managemen t	23-10-2019	7.5	Creative Cloud Desktop Application version 4.6.1 and earlier versions have Security Bypass vulnerability. Successful exploitation could lead to Privilege Escalation in the context of the current user. CVE ID: CVE-2019-8236	N/A	O-APP-MAC 041119/806
Inadequate Encryption Strength	23-10-2019	10	Adobe Acrobat and Reader versions 2019.012.20034 and earlier; 2019.012.20035 and earlier versions;	N/A	O-APP-MAC 041119/807

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			2017 earlie 2015 earlie 2015 earlie Insuff Encry Succe could featur conte user.	earlier versions; 2017.011.30143 and earlier versions; 2015.006.30497 and earlier versions; 2015.006.30498 and earlier versions have an Insufficiently Robust Encryption vulnerability. Successful exploitation could lead to Security feature bypass in the context of the current user. CVE ID: CVE-2019-8237						
mac_os_x										
Out-of- bounds Read	17-10-2019	4.3	version and e 2017 earlie 2015 earlie bound Succession of the could	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and				https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-APP-1 041119	_
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
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	5	2015.006.30503 and earlier have a cross-site scripting vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8160 Adobe Acrobat and Reader versions 2019.010.20100 and earlier; 2019.010.20099 and earlier versions; 2017.011.30140 and earlier version; 2017.011.30138 and earlier version; 2015.006.30495 and earlier versions; 2015.006.30493 and earlier versions have a Path Traversal vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	N/A	O-APP-MAC 041119/810
A			CVE ID : CVE-2019-8238		
Asus	a we are 5 04 -	G			
rog_zepnyru	s_m_gm501gs_	1117111W		1	
Improper Input Validation	20-10-2019	7.2	** DISPUTED ** The BIOS configuration design on ASUS ROG Zephyrus M GM501GS laptops with BIOS 313 relies on the main battery instead of using a CMOS battery, which reduces the value of a protection mechanism in which booting from a USB	N/A	0-ASU-ROG 041119/811
CV Scoring Sca	ole 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
			device is prohibited. Attackers who have physical laptop access can exhaust the main battery to reset the BIOS configuration, and then achieve direct access to the hard drive by booting a live USB OS without disassembling the laptop. NOTE: the vendor has apparently indicated that this is "normal" and use of the same battery for the BIOS and the overall system is a "new design." However, the vendor apparently plans to "improve" this an unspecified later time. CVE ID: CVE-2019- 18216		
avstar					
pe204_firmw	vare				
Improper Input Validation	23-10-2019	5	An issue was discovered on AVStar PE204 3.10.70 IP camera devices. A denial of service can occur on open TCP port 23456. After a TELNET connection, no TCP ports are open. CVE ID: CVE-2019-18382	N/A	O-AVS-PE20- 041119/812
Bitdefender					
box_firmwar	е				
Allocation of Resources Without	17-10-2019	4.9	An issue was discovered in Bitdefender BOX firmware versions before 2.1.37.37-	O-BIT-BOX 041119/813	
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	NCIIPC ID						
Limits or Throttling			34 that affects the general reliability of the product. Specially crafted packets sent to the miniupnpd implementation in result in the device allocating memory without freeing it later. This behavior can cause the miniupnpd component to crash or to trigger a device reboot. CVE ID: CVE-2019-12611								
Canonical	Canonical										
ubuntu_linu	x										
Out-of- bounds Write	28-10-2019	7.5	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution. CVE ID: CVE-2019- 11043	https://bugs. php.net/bug.p hp?id=78599, https://suppo rt.f5.com/csp /article/K754 08500?utm_s ource=f5supp ort&utm _medium=RSS	O-CAN-UBUN- 041119/814						
Improper Input Validation	17-10-2019	9	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For	https://securi ty.netapp.com /advisory/nta p-20191017- 0003/, https://suppo rt.f5.com/csp /article/K537 46212?utm_s	O-CAN-UBUN- 041119/815						
CV Scoring Sca (CVSS)	ale 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
			example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#\$((0xffffffff))" command. CVE ID : CVE-2019- 14287	ource=f5supp ort&utm _medium=RSS , https://www. sudo.ws/alert s/minus_1_ui d.html	
Use After Free	18-10-2019	6.8	In xsltCopyText in transform.c in libxslt 1.1.33, a pointer variable isn't reset under certain circumstances. If the relevant memory area happened to be freed and reused in a certain way, a bounds check could fail and memory outside a buffer could be written to, or uninitialized data could be disclosed. CVE ID: CVE-2019-18197	N/A	O-CAN-UBUN- 041119/816
Missing Release of Resource after Effective Lifetime	18-10-2019	7.2	In the Linux kernel before 5.3.4, a reference count usage error in the fib6_rule_suppress() function in the fib6 suppression feature of net/ipv6/fib6_rules.c, when handling the FIB_LOOKUP_NOREF flag, can be exploited by a local attacker to corrupt memory, aka CID-ca7a03c41753. CVE ID: CVE-2019-18198	N/A	O-CAN-UBUN- 041119/817
Use After	24-10-2019	5	archive_read_format_rar_r	N/A	O-CAN-UBUN-
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
Free			archiv mat_r befor after- ARCH situat	lata in ve_read_ car.c in li e 3.4.0 h free in a IIVE_FAI ion, rela	barchive as a use certain LED ted to	e -			041119	/818
			CVE I 1840	D : CVE- 8	2019-					
Cisco										
250_series_fi	250_series_firmware									
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interf Busin Mana allow remove conductive attack system is due prote based interf device exploy pethe in malic succe allow perform with the tarent system in the tarent sys	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative		N/A		O-CIS-2 041119	_	
CV Scoring Scal	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper Neutralizati on of Input During Web-page Generation ('Cross-site Scripting') Scripting') Improper Neutralizati on of Liput During Web-page Generation ('Cross-site Scripting') Cross-site Scripting') Improper Neutralizati on of Liput During Web-page Generation ('Cross-site Scripting') Cross-site Scripting') Inspection of Liput During Web-page Generation ('Cross-site Scripting') Improper Neutralizati on of Liput During Web-page Generation ('Cross-site Scripting') Inspection with the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718				commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
	Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')		4.3	based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	_

Weakness	Publish Date	cvss	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interf Busin Mana allow remove conducting attack system is due prote based interf device explo by pethe in malic succe allow perfor with the tauser he privil could configure communication device allow the tauser he privil could configure communication device the condition of the could configure condition device the condition of the could configure condition of the could configure condition of the condition of the condition of the could condition of the co	D : CVE-	ement sco Sma rt and ches con thentica er to ss-site ry (CSRF ffected ulnerabi fficient Cor the we ement n affecte acker co ulnerabil g a user o co follow cher to rary act lege leve ser. If the nistrative e attacker c cause a fice (DoS an affect	all uld ated, ility CSRF eb- ed uld lity of a ld ions el of ne ve er	N/A		0-CIS-3 041119	_
Improper Neutralizati on of Input During Web Page Generation	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,			co and uld	N/A		0-CIS-3 041119	_
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	te attack 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
('Cross-site Scripting')			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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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- 12718							
550x_series_	firmware									
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management				N/A		0-CIS-5 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			device explosion by per the immalice succes allow performithe tauser in the tauser in	D : CVE-	acker co alnerabil g a user of to follow a. A bloit cou cker to rary act lege leve aser. If the nistrative attacker cause a fice (DoS	ould lity of 7 a lld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and				N/A		O-CIS-5 041119	
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	NCIIPC ID
			subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
200_series_fi	irmware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-	N/A	O-CIS-200 041119/825

CV Scoring Scale

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID			D	Pate	:h	NCIIP	CID
			based information.							
			CVE I	D : CVE	2019-					
			12718							
300_series_fi	rmware									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specii page. could execu code affect acces based	nerability I interface Busines ged Swi I an unau ite attack act a cro cing (XSS st a user I interface rability ficient va supplied based in red device act o cl ious link equently fic web i A succe allow the atte arbite in the co red interface s sensiti I inform D: CVE- 8	ce of Ciscs Smart tches conthenticater to ss-site S) attack of the voce. The didation of the voce. An didation of the voce and access a context of face or ve brown ation.	co and uld ated, web- of the this che cloit cer to pt the	N/A		O-CIS-3 041119	
Improper Privilege Managemen	16-10-2019	10	Airon	nerabilit et Acces Softwai	s Points	;	N/A		O-CIS-A 041119	
	<u> </u>		· · · · · · · · · · · · · · · · · · ·							
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	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
t			remore unaute target elevate vulne insuff for ce affect attack vulne requestion the deprivil attack grant possil option attack informsome of the includent of the includent tack (DoS) assoc CVE I 1526	nerabilit	er to gain access to en with leges. The solution cess con Ls on an end exploit oy ecific UF ed AP. An allow the in access he elevated not be so to all guration ld allow ew sensing replaying the sable the sa	this the tive ace aues				
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	of Wind (CAPV) imple Airon	rol and Proceedings of the contraction of the contr	ccess Pos otocol on of Cis atalyst 9	ints sco 2100	N/A		O-CIS-A 041119	
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
			adjacent attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management during CAPWAP message processing. An attacker could exploit this vulnerability by sending a high volume of legitimate wireless management frames within a short time to an affected device. A successful exploit could allow the attacker to cause a device to restart unexpectedly, resulting in a DoS condition for clients associated with the AP. CVE ID: CVE-2019-15264							
Improper Input Validation	16-10-2019	2.1	A vulnerability in the bridge protocol data unit (BPDU) forwarding functionality of Cisco Aironet Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an AP port to go into an error disabled state. The vulnerability occurs because BPDUs received from specific wireless clients are forwarded incorrectly. An attacker could exploit this				N/A		O-CIS-A 041119	
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
			vulnerability on the wireless network by sending a steady stream of crafted BPDU frames. A successful exploit could allow the attacker to cause a limited denial of service (DoS) attack because an AP port could go offline. CVE ID: CVE-2019-15265		
aironet_156	0_firmware				
Improper Privilege Managemen t	16-10-2019	10	A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated, remote attacker to gain unauthorized access to a targeted device with elevated privileges. The vulnerability is due to insufficient access control for certain URLs on an affected device. An attacker could exploit this vulnerability by requesting specific URLs from an affected AP. An exploit could allow the attacker to gain access to the device with elevated privileges. While the attacker would not be granted access to all possible configuration options, it could allow the attacker to view sensitive information and replace some options with values of their choosing,	N/A	O-CIS-AIRO- 041119/830

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			including wireless network configuration. It would also allow the attacker to disable the AP, creating a denial of service (DoS) condition for clients associated with the AP. CVE ID: CVE-2019- 15260		
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol implementation of Cisco Aironet and Catalyst 9100 Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management during CAPWAP message processing. An attacker could exploit this vulnerability by sending a high volume of legitimate wireless management frames within a short time to an affected device. A successful exploit could allow the attacker to cause a device to restart unexpectedly, resulting in a DoS condition for clients associated with the AP. CVE ID: CVE-2019-	N/A	O-CIS-AIRO- 041119/831

Weakness	Publish Date	cvss	Description & CVE ID				Pato	:h	NCIIP	C ID
			1526	4						
Improper Input Validation	16-10-2019	2.1	bridg (BPD) functi Airon (APs) unaut attack port t disab vulne becau from client incorr could vulne wirel sendi crafte succe allow a limi (DoS) AP po	nerability of protocol (III) forward ionality of the Access could all thentical exer to call the attack of the Access are for rectly. A exploit prability exert exploit prability exert exploit prability exert exploit prability exert could the attack of th	ol data userding of Cisco as Points allow an ted, adjause an Aco an error and a ted and a ted an attack this on the cork by ady streames. Oloit coucker to a al of seroecause go offling	cent AP or ved s er am of A alld cause vice an	N/A		O-CIS-A 041119	
aironet_1800)_firmware									
Improper Privilege Managemen t	16-10-2019	10	Airon (APs) allow remo unaut target elevat vulne insuff	nerabilite Acces Software an unaute attacket deviced privication acceptation UR	es Points re could athentica ter to ga access t ce with leges. The is due to	ated, in to a he o	N/A		0-CIS-A 041119	
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	D	escription	ı & CVE II)	Pato	:h	NCIIP	CID
			vulne reque from a exploration attack grante possili option attack information of the include network would attack creati (DoS) associated (DoS) associated (DoS)	attacker could exploit this vulnerability by requesting specific URLs from an affected AP. An exploit could allow the attacker to gain access to the device with elevated privileges. While the attacker would not be granted access to all possible configuration options, it could allow the attacker to view sensitive information and replace some options with values of their choosing, including wireless network configuration. It would also allow the attacker to disable the AP, creating a denial of service (DoS) condition for clients associated with the AP. CVE ID: CVE-2019-15260						
Improper Input Validation	16-10-2019	2.1	A vulnerability in the bridge protocol data unit (BPDU) forwarding functionality of Cisco Aironet Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an AP port to go into an error disabled state. The vulnerability occurs because BPDUs received from specific wireless clients are forwarded incorrectly. An attacker				N/A		O-CIS-A 041119	
						er				

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
			vulne wirele sendir crafte succe allow a limi (DoS) AP po	d BPDU ssful exp the atta ted deni attack l rt could D: CVE-	on the rork by ady streames. cloit coucker to call of servecause go offling.	A ld cause vice an				
aironet_2800)_firmware									
Improper Privilege Managemen t	16-10-2019	10	Airon (APs) allow remote unaut target elevat vulne insuff for ce affect attack vulne from a explor attack the de privile attack grante possil option attack	A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated, remote attacker to gain unauthorized access to a targeted device with elevated privileges. The vulnerability is due to insufficient access control for certain URLs on an affected device. An attacker could exploit this vulnerability by requesting specific URLs from an affected AP. An exploit could allow the attacker to gain access to the device with elevated privileges. While the attacker would not be granted access to all possible configuration options, it could allow the attacker to view sensitive information and replace					O-CIS-A 041119	
CV Scoring Sca	le 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
			of their choosing, including wireless network configuration. It would also allow the attacker to disable the AP, creating a denial of service (DoS) condition for clients associated with the AP.		
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol implementation of Cisco Aironet and Catalyst 9100 Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management during CAPWAP message processing. An attacker could exploit this vulnerability by sending a high volume of legitimate wireless management frames within a short time to an affected device. A successful exploit could allow the attacker to cause a device to restart unexpectedly, resulting in a DoS condition for clients	N/A	O-CIS-AIRO- 041119/836

Weakness	Publish Date	cvss	D	escriptio	n & CVE II	D	Pate	ch	NCIIP	C ID
			CVE I 1526	D : CVE- 4	2019-					
Improper Input Validation	16-10-2019	2.1	bridg (BPD) functi Airon (APs) unaut attack port t disabi vulne becau from client incorr could vulne wirele sendi crafte succe allow a limi (DoS) AP po	nerability of protocol on ality of et Access could also denticate to case of go into the specific of the action of	ol data unding of Cisco is Points low an end, adjause an Arrown an errown and errown attack this on the error by ady streames. Oloit councker to coal of servecause go offling and the error and of servecause go offling and the error and the	cent P or ed am of A ld cause vice an	N/A		0-CIS-A 041119	
aironet_3800)_firmware									
Improper Privilege Managemen t	16-10-2019	10	Airon (APs) allow remor unaut target elevat vulne	nerabilit et Acces Softwar an unau te attack chorized ted device ted privi rability	s Points te could athentica ter to gai access t ce with leges. Tl	ated, in o a ne	N/A		0-CIS-A 041119	
CV Scoring Sca (CVSS)	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			affect attack vulne reque from explo attack the de privil attack grant possil option attack inform some of the include network would attack creati (DoS) associ	rtain UR ed device rability lesting special an affect it could a cer to gas evice wite eges. Whe cer woul ed acces ble confines, it cou cer to vice mation a options ir choos ding wire ork confid also all cer to dis ng a den condition iated wite D: CVE- 0	e. An I exploit by ecific UF eed AP. A allow th in access ch elevat nile the d not be s to all guration ald allow ew sensi nd repla with val ing, eless iguration ow the sable the hial of se on for cli th the Al	this RLs an e s to red the tive ace aues a. It				
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	Control of With CAPV imple Airon Accessallow adjace an affirestal result service.	nerability of and Preless Act WAP) presentation et and Coordinate an unaute ent attace fected de rt unexpecting in act ce (DoS) ulnerabi	rovision ccess Po- otocol on of Cis atalyst 9 (APs) co thentica- ker to ca vice to ectedly, denial o condition	ints sco 9100 ould ated, ause f	N/A		0-CIS-A 041119	
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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			mana CAPW proce could vulne high v wirele frame to an succe allow a devi unexp a DoS assoc	pper resorder resorde	during sage nattackethis by sending sement a short device. Start resulting for clitch the All start and	ng a nate time A ld cause				
Improper Input Validation	16-10-2019	2.1	bridg (BPD) functi Airon (APs) unaut attack port t disabi vulne becau from client incorr could vulne wirele sendi crafte succe allow	nerability of the protocol of	ol data unding of Cisco s Points low an end, adjause an Arcurs. The occurs Us received an attack this on the ork by ady stready streames. Oloit coucker to occurs.	cent P or ved er A ld cause	N/A		O-CIS-A 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			AP po	attack bort could D: CVE- 5	go offlin					
aironet_4800	_firmware									
Improper Privilege Managemen t	16-10-2019	10	Airon (APs) allow remo unaut target elevat vulne insuff for ce affect attack vulne reque from explo attack grant possil option attack inforr some of the includ netwo would attack (DoS)	nerabilited Accessoftware an unaute attack chorized deviced privicient accessoft an affect at could accessoft accessort accessort accessort accessort accessory access	s Points te could athentica ter to gai access to the with leges. The is due to the cess cor the An d exploit by ted AP. A allow the in access the elevate hile the d not be s to all guration ald allow the sto all guration drepla with val ing, teless tiguration ow the sable the hial of se ton for cl	ated, in o a he o he o this RLs an e s to ed tive tive lues n. It e AP, rvice ients	N/A		O-CIS-A 041119	_
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	D	escriptio	n & CVE I	D		Patc	h	NCIIP	CID
			CVE I 1526	D : CVE- 0	2019-						
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	Controf William (CAPV) imple Airon Access allow adjace an aff restair result service The vimproces could vulner high vimproces allow a deviation and a deviati	reless Ad WAP) promentation and Control of the and Control of the attack	rovision coess Pootocol on of Cisatalyst 9 (APs) continued the condition of Cisatalyst 9 (APs) condition of Cisatalyst 9 (APs) condition of legiting agement of a short device. The condition of the Art of the A	ints sco 9100 ould ated, ause f on. ue to er ang a nate time A ld cause ag in ients	N/A			O-CIS-A 041119	
aironet_1810	_firmware										
Improper Input Validation	16-10-2019	7.8	A vulnerability in the Point-to-Point Tunneling Protocol (PPTP) VPN packet processing functionality in Cisco				N/A			0-CIS-A 041119	
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
			Aironet Access Points (APs) could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Generic Routing Encapsulation (GRE) frames that pass through the data plane of an affected AP. An attacker could exploit this vulnerability by associating to a vulnerable AP, initiating a PPTP VPN connection to an arbitrary PPTP VPN server, and sending a malicious GRE frame through the data plane of the AP. A successful exploit could allow the attacker to cause an internal process of the targeted AP to crash, which in turn would cause the AP to reload. The AP reload would cause a DoS condition for clients that are associated with the AP.		
			15261		
aironet_1830	_firmware				
Improper Input Validation	16-10-2019	7.8	A vulnerability in the Point-to-Point Tunneling Protocol (PPTP) VPN packet processing functionality in Cisco	N/A	O-CIS-AIRO- 041119/844
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
			Aironet Access Points (APs) could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Generic Routing Encapsulation (GRE) frames that pass through the data plane of an affected AP. An attacker could exploit this vulnerability by associating to a vulnerable AP, initiating a PPTP VPN connection to an arbitrary PPTP VPN server, and sending a malicious GRE frame through the data plane of the AP. A successful exploit could allow the attacker to cause an internal process of the targeted AP to crash, which in turn would cause the AP to reload. The AP reload would cause a DoS condition for clients that are associated with the AP.		
			15261		
aironet_1850	_firmware				
Improper Input Validation	16-10-2019	7.8	A vulnerability in the Point-to-Point Tunneling Protocol (PPTP) VPN packet processing functionality in Cisco	N/A	O-CIS-AIRO- 041119/845
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	D	escription	a & CVE II	D	Pato	h	NCIIP	CID
Uncontrolle	Publish Date	CVSS	Airon (APs) unaut attack affect result servic The v insuff Gener Encap frame the da affect could vulne assoc AP, in conne PPTP sendi frame plane succe allow an int target which the Al reload condi are as CVE I 1526 A vuln Contr	the Access could all thenticate dericated device ing in a ce (DoS) ulnerability be interested AP. At exploit to rability be interested and properties at the attack of the All soful exploit to reload to the attack of the attack	s Points low an ed, rem use an e to relo denial o conditio lity is di lidation ng (GRE) as throu of an n attack this by a vulne a PPTP V an arbit ver, and icious G o the dat P. A loit cou cker to c ocess of o crash, would c ad. The cause a clients the liwith the course y in the rovision	ote ad, f on. ue to of agh er RE a ld cause the ause AP DoS hat e AP.	Patc	:h		
d Resource Consumptio n	16-10-2019	6.1	(CAPV imple Airon	reless Ac WAP) pro ementation et and Ca es Points	otocol on of Cis atalyst 9	sco 9100	N/A		0-CIS-A 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			allow adjact an affirestal result service mana CAPV procestould vulner high wirel frame to an succes allow a devunexy a DoS association and association association and association associatio	ran unauent attace fected de rt unexpeting in a ce (DoS) rulneraboper research vAP messessing. A exploit explo	ethentical exice to condition in a short device. The condition is agent as short device. The condition is a short device. The condition is a short device. The condition is a short device as a short device at a	er ing a nate t time A lld cause				
5500_wireles	ss_controllers_	firmw	are							
Improper Input Validation	16-10-2019	7.8	Secur mana Wirel (WLC allow remo denia condi devic exists proce delete	nerabilite Shell (gement less LAN s) Softwar an unaute attack lof servettion on a servettion to the control of	SSH) sest for Cisco Control are could athenticater to car ice (DoS an affect alnerabite the SSH an SSH	ler lated, use a l) eed lity	N/A		O-CIS-5 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			could vulne repeat connection device explositated multito the effect which DoS could be a could be	exploit exploit rability ratedly operations to exert to exert to exert to exert exer	this by ening Stockersful allow th haust sy initiating connect that are eminated esult in h.	SH ected e rstem g ions not				
catalyst_910	0_firmware			_						
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	Controf Wi (CAP) imple Airon Access allow adjacent are started to the view of	nerability reless Ad WAP) prementation and Control of the tand control of tand con	rovision coess Po otocol on of Cistallyst Garalyst Garaly	ints sco 9100 ould ated, ause f on. ue to er	N/A		0-CIS-C 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
			succe allow a dev unexp a DoS assoc	affected ssful expected to respectedly condition in the condition of the c	oloit councker to one start of the start of the start on for club, the A	ald cause ng in ients				
firepower_m	anagement_c	enter_2	600_fi	rmware	•					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execute code interf sensitinform	ple vuln eb-base gement Firepow gement) could a extra to co site scrit against cased m face. The ficient va- supplied based m face. An a exploit rabilitie face to cl A succes allow th te arbit in the co face or a cive, bro mation. D: CVE- 8	interfactiver Center Allow an I, remote induct a ipting (X a user of a anagement attacker these is by user of the attacker attack	e of (SS) of the ent e to of y the ent che afted loit ger to pt the	N/A		O-CIS-F 041119	
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	Des	criptio	n & CVE I	D	Pato	h	NCII	PC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the well manage Cisco F Manage (FMC) of auther attacke cross-s attack a web-ba interface vulnerations of the could evel be a could evel be a could a execute code in interface to the could a execute code in interface.	b-based ement could a ticated or to co ite scripagainst ased makes abilitie ding a ce to classification the co ce or action.	interfactiver Center Center Illow and remote and exter a user of an agementacker an agementacker of these actacker actac	e of (SS) of the ent e to of y the ent che afted loit ger to pt the	N/A		0-CIS-I 04111	
firenower ar	ppliance_7030) firmw								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple the well manage Cisco F Manage (FMC) e authen	b-based ement irepowement could a ticated er to co	interfac ver	e of	N/A		0-CIS-I 04111	
CV Scoring Sca	lle 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	D	escription	n & CVE II	D	Pato	ch	NCIIP	C ID
			web-linterf vulne insuff user-s web-linterf could vulne persu interf link. A could execu code i interf sensit inform CVE I	against based marabilities rabilities supplied based marabilities adding a marabilities allow that arbitrin the corace or active, brownation. B: CVE-8	anagemose se s are due lidation input b anagemo attacker these s by user of t ick a cra sful expl ae attack ary scri ntext of ccess wser-ba	ent e to of y the ent the ofted oit cer to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the				N/A		0-CIS-F 041119	
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	Pato	ch	NCIIP	C ID
			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 access sensitive, browser-based information. CVE ID: CVE-2019-				
			15269				
firepower_ap	pliance_7110_	firmw	are				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-	N/A		O-CIS-F 041119	
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	Des	cription	& CVE II	D	Pato	:h	NCIIP	CID
			15268							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple the web manage Cisco Fi Manage (FMC) c authent attacker cross-si attack a web-bar interface vulnera insuffice user-su web-bar interface could ex vulnera persuace interface could ex vulnera persuace interface could al execute code in interface sensitiv informa	ement in trepower the scrip against a sed marked marked marked marked marked marked ing a uncertainty and the correct or action.	nterface er low an remote aduct a oting (X a user of a user of are duction input by nagement idation input by nagement idation input by nagement tracker hese by liser of t ck a cra ful expl e attack ary scrip ntext of cess vser-bas	es of SS) of the ent e to of y the ent he fted oit er to pt the	N/A		O-CIS-F 041119	
firepower_ap	ppliance_7115	_firmw	are							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a			e of	N/A		0-CIS-F 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			attack web-l interf vulne insuff user-s web-l interf could vulne persu interf link. A could execu code interf sensit inform	rabilities ace. The rabilities ased marked marked marked marked marked marked marked ace. An ace ace to classed the arbitrin the contact of ace or active, brown ation. D: CVE-8	a user of an agemones are duralidation input be an agemone attacker attacker these as by user of the attacker ary script are script	e to of y the ent che afted oit ser to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by				N/A		O-CIS-F 041119	
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	Descr	iption & CVE I	D	Pato	:h	NCIIP	CID
			interface link. A su could allo execute a code in the interface sensitive informat	ng a user of to click a cracessful explow the attackarbitrary scrine context of or access, browser-basion.	afted loit ker to pt the				
firepower_m	anagement_ce	nter_v	rtual_app	oliance_firm	ware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the web- managen Cisco Fire Managen (FMC) co authentic attacker cross-site attack ag web-base interface vulnerab insufficie user-sup web-base interface could exp vulnerab persuadi interface link. A su could alle execute a code in th interface	nent interface epower nent Center uld allow and cated, remote to conduct a e scripting (X ainst a user of ed managem . These ilities are du not validation plied input be ed managem . An attacker bloit these ilities by ng a user of to cocessful explor ow the attack arbitrary scripte context of or access , browser-ba	e of (SS) of the ent e to of the ent che afted loit cer to pt the	N/A		0-CIS-F 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	C ID
			CVE I 1526	D : CVE- 8	2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execute code interf sensitinform	ple vulneblased gement Firepow gement oculd a chicated a chicated a cased marked based makes and a cased marked based marked a cased marked based marked based marked based marked a cased marked based	interface ver Center allow an l, remote nduct a ipting (X c a user of anagement is se s are du- alidation l input b anagement attacker these s by user of t ick a cra sful expl ne attack crary scri ontext of ccess wser-ba	e of (SS) of the ent e to of y the ent che afted oit cer to pt the	N/A		0-CIS-F 041119	
firepower_ma	anagement_c	enter_2	000_fi	rmware						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote				N/A		O-CIS-F 041119	
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	D	escriptio	n & CVE I	D		Patc	h	NCIIP	C ID
Scripting')			cross attacl web-l interf vulne insuff user- web-l interf could vulne persu interf link. A could execu code interf sensif inform	ker to co-site scrite scribilities and scribe scribilities adding a successallow that arbitration the compation. D: CVE-8	ipting (X a user of anagements s are du alidation l input b anagement attacker these s by user of to ick a crassful explance attacker ick a crassful explance ary scription text of ccess wser-ba	e to of the ent of y the ent of the ofted loit ser to pt of the often					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multi the w mana Cisco Mana (FMC authe attacl cross attacl web- interf vulne insuff user- web- interf could	N/A			O-CIS-F 041119				
CV Scoring Sca (CVSS)	le 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
			vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15269		
firepower_m	anagement_ce	nter_1	000_firmware		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based	N/A	O-CIS-FIRE- 041119/861

Weakness	Pub	lish Date	CVSS	S Description & CVE ID					Pato	h	NCIIP	C ID
				inforn	nation.							
				CVE I 1526	D : CVE- 8	2019-						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-1	.0-2019	3.5	the wimana Cisco Mana (FMC) auther attack cross attack web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuinterf sensit inform	ple vulnerebbased gement Firepower gement Could a conticated a car to consider script against cased managed ma	d interface ver Center illow an , remote nduct a pting (X a user of anageme attacker these s by user of t ick a cra sful expl ne attack rary scri ntext of ccess wser-ba	e of SSS) of the ent e to of y the ent he afted oit ter to pt the	N/	'A		0-CIS-F 041119	
Improper	nagen	nent_ce	nter_35	00_firmware								
Neutralizati				Multiple vulnerabilities in the web-based								
on of Input During Web Page	16-1	.0-2019	3.5	management interface of Cisco Firepower Management Center				N/	/A		0-CIS-F 041119	
Generation				(FMC) could allow an								
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	D	escriptio	n & CVE I	D	-	Patch		NCIIF	CID
('Cross-site Scripting')			attack cross attack web-k interf vulne insuff user- web-k interf could vulne persu interf link. A could execu code interf sensif inform	enticated ker to corsite scrit scrit scrit ker to corsite scrit ker against based made. The erabilities adding a face. An allow the erabilities adding a face to classed mucces allow the erabilities arbitration the corsitive, brown ation. ED: CVE. 18	induct a ipting (X ta user of anagement of these attacker of these attacker of these attacker of the attacker of these attacker of these attacker of these attacker of these attacker of the a	ess) of the ent e to of y the ent che afted oit ser to pt the					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multi the w mana Cisco Mana (FMC authe attacl cross attacl web-l interf vulne insuff user- web-l interf	N/A			O-CIS-F 041119				
CV Scoring Scal	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	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15269		
firepower_ap	ppliance_7125	_firmw			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access	N/A	O-CIS-FIRE- 041119/865

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	n & CVE I	D		Pato	h	NCIIP	C ID
			inform CVE I 1526 Multi	tive, brownation. D: CVE- 8 ple vulno eb-baseo	2019- erabiliti						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Cisco Mana (FMC) auther attack cross-attack web-k interfection of the could vulne persure interfection of the could execute code in the code in th		Center allow an apting (X a user of an agemontate attacker these is by user of the attacker a	es (SS) of the ent e to of y the ent che fted loit ser to pt the	N/	A		O-CIS-F 041119	
firepower_ma	anagement_c	enter_4	1	00							
Improper Neutralizati on of Input During Web Page	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center				N/	A		O-CIS-F 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3-4	5-6		6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
Generation ('Cross-site Scripting')			auther attack cross attack web-linterf could vulne persuinterf link. A could executed interf sensitinform	could a enticated er to consider scrip scrip scrip sased material supplied based material supplied based material supplied based material supplied based material successive allow that arbitration the consider specific supplied based material successive allow that arbitration the consider specific specific specific successive, brown ation. D: CVE-8	, remote nduct a pting (X a user of anagement se s are ductal alidation input by anagement attacker these s by user of t ick a cra sful expl ne attack rary scri ntext of ccess wser-ba	esss) of the ent e to of of y the ent the oft oft the oft the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross attack web-l interf vulne insuff user-s	ple vulne deb-based gement (Firepow gement () could a enticated ker to con- site scri k against based ma face. The erabilities ficient value based ma	d interface ver Center illow an , remote nduct a pting (X a user of anageme se s are due lidation	e of SSS) of the ent e to of y the	N/A		O-CIS-F 041119	
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
			interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-		
		_	15269		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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	N/A	O-CIS-FIRE- 041119/869

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
			sensitinform		wser-ba					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-sweb-linterf could vulne persuinterf link. A could execut code interf sensitinform CVE I 1526		interface ver Center allow an anduct a pting (X a user of anagement input b anagement attacker these s by user of t ick a crassful explance attack ary scri- intext of ccess wser-ba	e of (SS) of the ent e to of y the ent che afted loit ser to pt the	N/A		O-CIS-F 041119	
firesight_man	nagement_ce	nter_15	00_firr	nware						
Improper Neutralizati on of Input During Web	16-10-2019	3.5	the w	ple vulne eb-basee gement Firepow	d interfac		N/A		0-CIS-F 041119	
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
Page Generation ('Cross-site Scripting')			(FMC) auther attack cross attack web-linterf vulne insuff user-stand vulne persuinterf link. A could execute code interf sensitinform	gement (a) could a cou	illow an , remote nduct a pting (X a user of anagement of these is by user of these attacker ary scriptext of exess wser-ba	ess) of the ent e to of y the ent he ofted oit er to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff	ple vulne eb-based gement if Firepow gement (i) could a enticated ker to con- site scri k against cased ma face. The rabilities ficient va supplied	d interface ver Center illow an , remote nduct a pting (X a user o anageme se s are du ilidation	e of (SS) of the ent e to	N/A		O-CIS-F 041119	
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	D	escriptio	n & CVE II)	Pato	h	NCIIP	CID
			interf could vulne persu interf link. A could execu code i interf sensit inform	exploit rabilitie ading a face to classed the arbitration the control accordance or ac	attacker these s by user of t ick a cra sful expl ae attack rary scri ntext of ccess wser-ba	he fted oit er to pt the				
			1526							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multithe wana Cisco Mana (FMC) auther attackers attackers web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could	ple vulne eb-based gement Firepow gement (a could a nticated er to could a ser to could a success allow the arbitic	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement is are duction input by anagement attacker these is by user of t ick a crassful explant	es of SS) of the ent e to of y the ent he fted oit er to	N/A		0-CIS-F 041119	

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the interface or access sensitive, browser-based information.		
			CVE ID : CVE-2019- 15268		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269	N/A	O-CIS-FIRE- 041119/874
firepower_ap	pliance_7120	_firmw	are		
Improper Neutralizati on of Input	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of	N/A	O-CIS-FIRE- 041119/875
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Mana (FMC) auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execut code interf sensitinform	Firepow gement () could a could a could a could a conticated a conticated a could a co	Center Illow an , remote nduct a pting (X a user of anageme s are due ilidation input by anageme attacker these s by user of t ick a cra sful expl ae attack ary scri ntext of ccess wser-bas	esss) of the ent e to of y the ent he ofted oit er to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross- attack web-l interf vulne	ple vulne eb-based gement (Firepow gement () could a enticated ker to con sare scri k against cased ma face. The rabilities	d interface ver Center Illow an , remote nduct a pting (X a user c anageme se s are due	e of (SS) of the ent	N/A		O-CIS-F 041119	
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

interface. An attacker could exploit these vulnerabilities by persuading a user of the interface of 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, browser-based information. CVE ID: CVE-2019-15269 The power_appliance_7010_firmw====================================	Weakness	Publish Date	CVSS	De	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting') 16-10-2019 3.5 Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit				web-b interfa could vulner persua interfa link. A could execut code i interfa sensit inform	ased make ace. An ace to classification the contact of the contact	anagemonttacker these s by user of to ick a cra sful expl ne attack rary scri ntext of ccess wser-ba	he fted oit eer to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting') 16-10-2019 Authorized Apart Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit	firepower_ap	ppliance_7010	_firmw								
	Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	3.5	the we manage Cisco Manage (FMC) auther attack cross-attack web-b interfavulner insuffi user-s web-b interfaculd vulner persua interfalink. A	eb-based gement could a nticated er to co site scri against ased made. The cient valuabilitie ased made as ased made as as as as a succession	d interface ver Center illow an I, remote nduct a pting (X I a user of anageme se s are du lidation input b anageme attacker these s by user of t ick a cra sful expl	e of SS) of the ent e to of y the ent he fited oit	N/A			

(CVSS)

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pato	h	NCIIP	C ID
			code interf sensitinform CVE I 1526	ite arbitrin the co face or active, brown mation. D: CVE- B	ntext of ccess wser-ba 2019-	the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC author attack cross attack web-linterficulty web-linterfi	reb-based gement (Firepower gement) could a co	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement input be anagement input be are attacker intext of ceess waser-ba	e of (SS) of the ent e to of y the ent che afted oit cer to pt the	N/A		O-CIS-F 041119	
firepower_ap	pliance_837	'0_firmv	vare							
Improper Neutralizati	16-10-2019	3.5		ple vulno eb-baseo		es in	N/A		O-CIS-F	IRE-
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
on of Input During Web Page Generation ('Cross-site Scripting')			Cisco Mana (FMC authe attack cross- attack web-l interf vulne insuff user web-l interf could vulne persu interf link. A could execu code i inform CVE I 1526		Center allow an an are duct a pting (X a user of an agement attacker attack	esss) of the ent e to of y the ent he fted oit ter to pt the			041119	/879
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross attack web-k interf	ple vulne eb-based gement (Firepow gement () could a enticated ker to co -site scri k against based ma face. The	d interface ver Center illow an , remote nduct a pting (X a user of anagements	e of (SS) of the ent	N/A		0-CIS-F 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			user web interficould vulne persu interfilink. A could execu code interfisensit	ficient vasupplied based made. An a exploit erabilitie ading a face to classification the conface or a tive, bromation.	l input b anageme attacker these s by user of t ick a cra sful expl ne attack cary scri ontext of ccess	y the ent che of the ent cer to pt the				
			CVE I 1526	D : CVE	-2019-					
firepower_m	anagement_ce	nter_1	600_fi	rmware	•					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf web-linterf could vulne persuinterf	ple vuln reb-base gement Firepow gement) could a enticated ker to co -site scri k against based m face. The brabilitie ficient va supplied based m face. An a exploit brabilitie rabilitie ading a face to cl	d interfactiver Center Allow an I, remote adjusting (X) I a user of an agement attacker attacker attacker at a craft a	e of SSS) of the ent e to of of y the ent	N/A		O-CIS-F 041119	
CV Scoring Sca	le 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
			could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. CVE ID: CVE-2019-15268		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269	N/A	O-CIS-FIRE- 041119/882

Weakness	Publish Date	CVSS	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attack web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuinterf sensitinform CVE I	ple vulne eb-based gement in the contact of a success allow the tearbitries or accive, brownation. P: CVE-8	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement input by anagement attacker these is by user of t ick a cra sful expl are attack vary scri- ntext of ccess wser-bas	e of SSS) of the ent e to of y the ent the oft the to the to	N/A		0-CIS-F 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management				N/A		O-CIS-F 041119	
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
			interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15269		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the	N/A	O-CIS-AMP 041119/885

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizati on of Liput During Web Scripting') Improper Neutralizati on Other Country Countr	Weakness	Publish Date	cvss	Description	& CVE ID		Patc	h	NCIIP	C ID
the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-				link. A successicular could allow the execute arbitrace or acceptance or acceptance of the continuation of the continuation of the continuation.	ful exploit e attacker to ary script ntext of the cess vser-based					
15269	Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	3.5	the web-based management in Cisco Firepower Management Company (FMC) could all authenticated, attacker to concross-site scrip attack against a web-based mainterface. These vulnerabilities insufficient valuser-supplied web-based mainterface. An accould exploit the vulnerabilities persuading a uninterface to click in the concould allow the execute arbitration code in the concinterface or accessitive, brown information.	nterface of er low an remote aduct a oting (XSS) a user of the nagement er are due to idation of input by the nagement execute by eser of the ck a crafted ful exploit e attacker to ary script execute of the cess exer-based	e N/	A			_

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firepower_ap	ppliance_8130	firmw	are		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268	N/A	O-CIS-FIRE- 041119/887
Improper Neutralizati on of Input During Web Page	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center	N/A	O-CIS-FIRE- 041119/888
Generation ('Cross-site Scripting')			(FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS)		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to conduct cross-site scripting attacks. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click	N/A	O-CIS-SPA1- 041119/889

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

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- 12702 A vulnerability in the webbased management interface of Cisco SPA122 ATA with Router Devices could allow an unauthenticated, adjacent attacker to conduct cross-site scripting attacks. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by sending malicious input to the affected software through crafted DHCP requests, and then 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 affected interface or access sensitive, browser-based information. CVE ID : CVE-2019-12703	Weakness	Publish Date	CVSS	De	scriptio	n & CVE II	D	Pato	h	NCIIP	CID
based management interface of Cisco SPA122 ATA with Router Devices could allow an unauthenticated, adjacent attacker to conduct cross-site scripting attacks. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software through crafted DHCP requests, and then 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 affected interface or access sensitive, browser-based information. CVE ID: CVE-2019-				exploit attacked arbitrat context interfat sensititinform	attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. CVE ID: CVE-2019- 12702 A vulnerability in the web- based management						
	Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	2.9	based interfal ATA who could a unauth attacked site scrivulner insufficuser-site web-basinterfal softwal could evulner malicidaffecte crafted and the user to A succeallow the execution code in affecte access based in the code in the code in affecte access based in the code in the c	manage ce of Cith Roulallow and enticate of the conting ability cient valuability ous input of the continuation of the attact of the attact of the attact of the attact of the continuation of the continuatio	ement is co SPA atter Devian ted, adja nduct crattacks. is due to alidation anagement in the contract of the context of face or ve, brow ation.	122 ices cent coss- The of y the ent ed ing link. ould pt the	N/A			

(CVSS)

Weakness	Publish Date	cvss	D	escription	ո & CVE II	D	Pat	ch	NCIIP	C ID
Information Exposure	16-10-2019	4	based interf Series Adapt allow remother to files of The vimpro in the mana attack vulne crafted web-linterf device exploattack conte on the result of series.		ement sco SPA Telepho As) coul enticate er to vie of arbitra ected de lity is di ut valida sed interface d exploit by sendi st to the anagemo affecte essful allow th trieve th bitrary f possibly te disclo formatic	100 one d d, ew ary vice. ue to ation e. An athis ag a ent d e files y sure	N/A		0-CIS-S 041119	
Information Exposure	16-10-2019	4	CVE ID: CVE-2019-12704 A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to unsafe handling of user credentials. An attacker could exploit this vulnerability by viewing				N/A		O-CIS-S 041119	
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
			portions of the web-based management interface of an affected device. A successful exploit could allow the attacker to access administrative credentials and potentially gain elevated privileges by reusing stolen credentials on the affected device. CVE ID: CVE-2019-12708		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-	N/A	O-CIS-SPA1- 041119/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15240		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-	N/A	O-CIS-SPA1- 041119/894
			15241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of	N/A	O-CIS-SPA1- 041119/895

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			web-linterficould vulne auther based interficrafter affect succe allow execution with a Note: manalenable	supplied based made. An a exploit of rabilities on ticating and a requested devices ful expension the arbitral elevated. The websel gement is early de	anagement these is by in the sending is stated and in the courant cours ary coding interface fault.	web- ld e ges.				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multicisco Analo Adapt allow adjace execu with o The v to impuser-s web-l interf could vulne authe based interf crafte affect succe	ple vulne SPA100 og Teleph ters (ATA an authorite arbitre elevated ulnerabit proper v supplied pased ma face. An a exploit to rabilities at request ed request ed device ssful exp	erabilition Series none As) coul enticate elker to cary cod privileg elities ar calidation input to anagement these es by eg to the ement sending sts to an e. A ploit cou	d d, e ges. e due n of o the ent	N/A		O-CIS-S 041119	
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	Pul	blish Date	e CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID	
				with Note: mana enabl	ite arbiti elevated The wel igement led by de (D: CVE	privileg b-based interfac efault.	ges.					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-	10-2019	5.2	Multi Cisco Analo Adap allow adjac execu with The v to im user- web- interi could vulne auther based interi crafte affect succe allow execu with Note: manalo	log Telephone pters (ATAs) could w an authenticated, cent attacker to cute arbitrary code n elevated privileges. vulnerabilities are due mproper validation of r-supplied input to the p-based management rface. An attacker ld exploit these nerabilities by nenticating to the web- ed management rface and sending ted requests to an cted device. A ressful exploit could w the attacker to cute arbitrary code n elevated privileges. e: The web-based nagement interface is bled by default. SID: CVE-2019-			0-CIS-S 041119				
Improper Restriction of Operations	16-	10-2019	5.2	Cisco Analo	ple vuln SPA100 og Telepl ters (AT	Series hone		N/A		O-CIS-SPA1- 041119/898		
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	D	escription	ո & CVE II	D	Pate	ch	NCIIP	CID
within the Bounds of a Memory Buffer			execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web- based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019- 15245							
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2				N/A		O-CIS-S 041119		
CV Scoring Scal	0-1	1-2	2-3	nticating 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15246		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default.	N/A	O-CIS-SPA1- 041119/900

4-5

5-6

6-7

7-8

8-9

9-10

1-2

0-1

2-3

CV Scoring Scale

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019- 15247		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-	N/A	O-CIS-SPA1- 041119/901
			15248		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due	N/A	0-CIS-SPA1- 041119/902

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			user-s web-linterf could vulne authe based interf crafte affect succe allow execu with e Note: mana enabl	proper very supplied based made. An adexploit for a carbilities and adexided a carbitrate arbitrate arbitr	input to anagement attacker these is by g to the ement sending ists to an e. A ploit counties cary code privilego- based interface fault.	o the ent web- ld ess.				
				D : CVE- 9	2019-					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapt allow adjace execu with a to impuser-s web-b interficould vulne auther based interficrafte	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A			N/A		0-CIS-S 041119	
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
			allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019- 15250		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15251	N/A	O-CIS-SPA1- 041119/904
Improper Restriction of	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone	N/A	0-CIS-SPA1- 041119/905
CV Scoring Sca (CVSS)	ole 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escription	1 & CVE II	D	Pato	:h	NCIIP	C ID
Operations within the Bounds of a Memory Buffer			allow adjace execu with execution web-binterficuld vulne auther based interficrafte affect succe allow execution with execution with execution with execution and enable	ters (ATA an author ent attace te arbitre elevated rulnerabi proper v supplied based ma ace. An a exploit in rabilities anticating d manage ace and a ed reques ed devic ssful exp the attace the arbitre elevated The web gement i ed by de D: CVE- 2	enticated cher to carry code privileg dilities are calidation anagement attacker these attacker to carry code privileg obased interfaced fault.	d, e ges. e due n of o the ent web-				
Information Exposure	16-10-2019	4	based interf Series Adapt allow remote an aff vulne improcessing An att this v	A vulnerability in the web-based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper restrictions on configuration information. An attacker could exploit this vulnerability by sending a request to an			N/A		O-CIS-S 041119	
			<u> </u>							

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected device through the web-based management interface. A successful exploit could allow the attacker to return running configuration information that could also include sensitive information. CVE ID: CVE-2019-15257		
Improper Input Validation	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper validation of user-supplied requests to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to cause the device to stop responding, requiring manual intervention for recovery. CVE ID: CVE-2019-15258	N/A	O-CIS-SPA1- 041119/907
spa112_firm	ware				

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interf Series Adapt allow remore conduscript vulne insuff user-s web-linterf softw could vulne persua craff exploattack arbitr conte interf sensit inform CVE I	merability in an authorise attack act crossing attack actions are of the ace of the ace of the action action action action action action action action action action. D: CVE-2	ement sco SPA Telepho As) coulcenticate er to -site cks. The didation input by anageme e affecte attacker this by user to c A succe allow th ecute ot code i affected ccess wser-bas	100 one d d, of y the ent ed click ssful e	N/A		0-CIS-S 041119	
Information Exposure	16-10-2019	4	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to view the contents of arbitrary files on an affected device. The vulnerability is due to improper input validation in the web-based management interface. An				N/A		0-CIS-S 041119	
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	1	NCIIPC	ID
			attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to retrieve the contents of arbitrary files on the device, possibly resulting in the disclosure of sensitive information. CVE ID: CVE-2019-12704				
Information Exposure	16-10-2019	4	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to unsafe handling of user credentials. An attacker could exploit this vulnerability by viewing portions of the web-based management interface of an affected device. A successful exploit could allow the attacker to access administrative credentials and potentially gain elevated privileges by reusing stolen credentials on the affected device. CVE ID: CVE-2019-12708	N/A		O-CIS-SP 041119/	
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	D	escription	ո & CVE II	D	Pate	:h	NCIIP	CID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapta allow adjace execution with execution with execution auther based interference allow execution with execution with execution with execution and enable CVE I		Series none As) coulcenticate ker to cary code privileg lities are alidation input to anagement attacker these s by g to the verent sending ests to an e. A oloit cou cker to cary code privileg o-based interface fault.	d d, e ges. e due n of o the ent ld e ges.	N/A		0-CIS-S 041119	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	CVE ID: CVE-2019- 15240 Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management				N/A		O-CIS-S 041119	
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	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
			could vulne authe based interf crafte affect successible with 6 Note: mana enable CVE I		these s by g to the vertical general g	web- ld e ges.				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	CVE ID: CVE-2019- 15241 Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code		N/A		0-CIS-S 041119			
			with 6	elevated	privileg	es.				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Note: The web-based management interface is enabled by default.		
			CVE ID : CVE-2019- 15242		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15243	N/A	O-CIS-SPA1- 041119/914
Improper Restriction of Operations within the Bounds of a	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to	N/A	O-CIS-SPA1- 041119/915
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	D	escriptio	n & CVE I	D	P	atch	NCIIF	PCID
Memory Buffer			with of the victor interfector of the could vulne auther for affect succes allow executivith of Note: manalenable	elevated rulnerab proper vesupplied based managed and requed devices and requed devices ful experienced the arbitral rule arbitr	s by g to the ement sending sts to an ce. A cloit cou cker to rary cod privileg b-based interface efault.	ges. e due n of the ent web-				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapa allow adjace execu with o The v to impuser- web-l interf could vulne auther based	SPA100 og Telepl ters (AT an auth ent attac ite arbiti elevated proper v supplied based m face. An a exploit erabilitie enticatin d manage	hone As) coul enticate cker to rary cod privileg ilities ar validatio l input to anageme attacker these s by g to the	d d, e ges. e due n of o the ent	N/A		O-CIS-S 041119	
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

Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations within the Bounds of a Memory Buffer 16-10-2019 Improper Restriction of Operations with elevated privileges. The wulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15246	Weakness	Publish Date	cvss	Descripti	Pato	h	NCIIP	CID		
Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web- based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-				affected dev successful e allow the at execute arbi with elevate Note: The w management enabled by c	ice. A Exploit cou Exploit cou Exploit cod Explor Exploit cod Exploit cod Exploit cod Exploit cod Exploit cod Exp	ld e ges.				
	Restriction of Operations within the Bounds of a Memory	16-10-2019	5.2	Cisco SPA10 Analog Tele Adapters (A allow an aut adjacent att execute arbi with elevate The vulnera to improper user-supplie web-based in interface. Ar could exploi vulnerabilit authenticati based mana interface an crafted requ affected dev successful e allow the att execute arbi with elevate Note: The w managemen enabled by o	O Series phone TAs) coul henticate acker to trary cod d privileg bilities ar validatio ed input to management attacker to these es by mg to the gement d sending ests to an ice. A exploit couracker to trary cod d privileg eb-based t interfactlefault.	d d, e ges. e due n of o the ent ld e ges.	N/A			

(CVSS)

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapta allow adjace executive with or to impuser web-linterficuld vulner auther based interficrafter affect succe allow executive with or Note: manalenable	ple vulne SPA100 og Telephters (ATA an authorite arbitre elevated proper volumerabilities arbilities and exploit for arbilities arbilities arbitre arbitre ed devices ful experte arbitre elevated The websel gement is ed by de D: CVE-7	Series none As) coulcenticate ker to cary code privileg lities are alidation input to an agement sending sts to an e. A coloit coursel code privileg obased interface fault.	d d, e ees. e due n of o the ent ld ees.	N/A		0-CIS-S 041119	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapt allow adjact execu with o The v to imp	ple vulne SPA100 og Teleph ters (ATA an autho ent attac elevated ulnerabi proper v supplied pased ma	Series none As) coulcenticate ker to eary code privileg lities are alidation input to	d d, e ees. e due n of o the	N/A		0-CIS-S 041119	
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	·				Pato	:h	NCIIP	CID
			interface. An attacker could exploit these vulnerabilities by authenticating to the web- based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019- 15248 Multiple vulnerabilities in Cisco SPA100 Series							
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapt allow adjace execu with earth of the vinterf could vulne auther based interf crafte affect succes allow execu	•	Series none As) could enticated ker to cary code privileg lities are alidation input to anagement see by g to the vertex to an eloit could ker to cary code cary code cary code could be anagement see	d d, e ges. e due n of o the ent web-	N/A		O-CIS-Si 041119	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Note: The web-based management interface is enabled by default.		
			CVE ID : CVE-2019- 15249		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15250	N/A	O-CIS-SPA1- 041119/921
Improper Restriction of Operations within the Bounds of a	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to	N/A	O-CIS-SPA1- 041119/922
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	D	escriptio	n & CVE I	D		Patc	h	NCIIF	CID
Memory Buffer			with of the victor interfector of the could vulne auther for affect succes allow executive with of Note: manalenable	elevated rulnerab proper vesupplied based made. An a exploit erabilitie entication I manage ace and ed reque ed devices ful experience arbitrate arbitrate arbitrate devated. The well gement ed by de D: CVE-	s by g to the ement sending sts to an ce. A cloit cou cker to rary cod privileg b-based interface	es. e due n of the ent ld es.					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adap allow adjace execu with o The v to imp user- web-l interf could vulne authe baseo	SPA100 og Telepl ters (AT an auth ent attac te arbiti elevated rulnerab proper v supplied based m face. An a exploit rabilitie	hone As) coul enticate cker to rary cod privileg ilities ar validatio l input to anageme attacker these s by g to the	d d, e ees. e due n of o the ent	N/A			O-CIS-S 041119	
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
			crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15252		
Information Exposure	16-10-2019	4	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper restrictions on configuration information. An attacker could exploit this vulnerability by sending a request to an affected device through the web-based management interface. A successful exploit could allow the attacker to return running configuration information that could also include sensitive information. CVE ID: CVE-2019-15257	N/A	O-CIS-SPA1- 041119/924
Improper Input Validation	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco SPA100	N/A	0-CIS-SPA1- 041119/925
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
			Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper validation of user-supplied requests to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to cause the device to stop responding, requiring manual intervention for recovery. CVE ID: CVE-2019- 15258		
ngips_virtual	_appliance_fir	mware			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the	N/A	O-CIS-NGIP- 041119/926

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pate	ch	NCIIP	C ID
			interf could vulne persu interf link. A could execu code i interf sensit inform	exploit frabilities ading a rading a rading a rading a rading a radiow that arbitrate arbitrate or accive, brown ation. D: CVE-8	attacker chese s by user of t ick a cra cful expl e attack ary scri ntext of ccess wser-ba					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attackers attackers web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuing code in the could execuing the could execuing the could execuing the could execuing the code in the could execuing the code in the could execuing the code in the	ple vulne eb-based gement of could a nticated are to consider to a sed marked based	dinterface ver Center Illow an premote induct a pting (X a user of anagement is are due lidation input by anagement input by anagement itacker these is by user of t ick a cra isful expl ary scriintext of	es of established site of the ent established site of the	N/A		O-CIS-N 041119	
CV Scoring Sca	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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
C			inforr CVE I 1526	ive, brov nation. D : CVE- 9		sed				
nrepower_ap	pliance_8390	_firmw	1							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attack web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuinterf sensitinform CVE I 1526		dinterface ver Center llow an , remote nduct a pting (X a user of anagement input by anagement attacker these is by user of the ick a cran input explained attacker attacker of the cran input explained attacker ary scrip intext of coess wser-base	es of es of esto of the ent esto of y the ent the fted oit ter to pt the sed	N/A		O-CIS-F 041119	
Improper Neutralizati on of Input During Web Page	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center				N/A		0-CIS-F 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
Generation ('Cross-site Scripting')			(FMC author attack cross attack web-linters web-linters could vulner inters inters could execute code inters sensitinform CVE I	(FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269						
firepower_ap	pliance_8270	_firmw	are							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wanta Cisco Mana (FMC auther attack cross attack web-interference of the control of the cont	ple vuln reb-base gement Firepow gement) could a reticated ker to co -site scri k against based m face. The rabilitie	interface ver Center allow an l, remote nduct a ipting (X t a user of anagements ese s are du	e of (SS) of the ent	N/A		O-CIS-F 041119	
CV Scoring Sca	le 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	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268 Multiple vulnerabilities in the web-based							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiputhe with manage (FMC) auther attack web-binterf vulne insuff user-sweb-binterf could vulne persuinterf link. A could execu	ple vulne	Interface ver Center Illow an premote nduct a pting (X a user of anagement in a user of anagement in put by anagement in put by anagement in put by anagement in a user of t ick a cra ick a cra ick a cra ick a cra ick a cra ick a cra ick a cra	e of SS) of the ent e to of y the ent he fted oit eer to pt	N/A		0-CIS-F 041119	
CV Scoring Sca	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	D	escription	& CVE II	D	Pato	h	NCIIP	CID
			sensit	ace or active, brown		sed				
			CVE I 1526	D : CVE- 9	2019-					
firepower_m	anagement_ce	nter_4	500_fi	rmware						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attack cross-attack web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execute code interf sensitinform	ple vulne eb-based gement of could a nticated er to consider the consideration of the arbitration the consideration. D: CVE-8	ter Center Center Illow an remote nduct a pting (X a user of a user of input by anageme stacker chese s by user of t ick a cra ful expl e attack ary scri ntext of cess wser-bas	e of SSS) of the ent e to of y the ent he afted oit ter to pt the	N/A		O-CIS-F 041119	
Improper Neutralizati on of Input During Web	16-10-2019	3.5	the w mana	ple vulne eb-based gement i Firepow	d interface		N/A		0-CIS-F 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
Page Generation ('Cross-site Scripting')			(FMC author attack cross attack web-linterformal could web-linterformal could execute code interformal code interform	gement) could a enticated ker to co -site scri k against based m face. The erabilitie ficient va supplied based m face. An a exploit erabilitie rabilitie ading a face to cl A succes allow th ite arbiti in the co face or a tive, bro mation. D: CVE- 9	allow an l, remote and ipting (X ta user of an agement attacker these attacker of the attacker attacker attacker attacker attacker acray scription text of access weer-ba	ess) of the ent e to of y the ent the afted loit ser to pt the ent				
firepower_ap	pliance_8250	_firmw	are							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attacl cross attacl web- interf	ple vuln reb-base gement Firepov gement) could a enticated ker to co -site scri k against based m face. The	d interfactiver Center allow an I, remote induct a ipting (X t a user of anagements	e of (SS) of the ent	N/A		0-CIS-F 041119	
CV Scoring Sca	le 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	D	escription	ı & CVE II	D	Patc	h	NCIIP	C ID
			user-s web-k interf could vulne persu interf link. A could execu code i interf sensit inforr	icient va supplied based ma face. An a exploit t rabilities ading a u face to cli A success allow th te arbitr in the con face or ac cive, brow nation.	input by anagement attacker these is by user of t ick a cra sful expl are attack ary scrip ntext of ccess wser-bas	y the ent che of the ent cer to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC) authe attack cross- attack web-k interf vulne insuff user-s web-k interf could vulne persu interf link. A could	ple vulne eb-based gement in Firepow gement (in) could a nticated resite scription cased managed face. The rabilities ficient value assed managed face. An anaged exploit the rabilities ading a unique and face to climate and allow the te arbitres	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement is are duction input by anagement attacker these is by user of t ick a cra sful expl	e of (SS) of the ent e to of y the ent the ifted oit cer to	N/A		0-CIS-F: 041119	

Weakness	Publis	h Date	cvss	D	escriptio	n & CVE I	D		Pato	h	NCIIP	C ID		
				code in the context of the interface or access sensitive, browser-based information.										
				CVE I 1526	D : CVE- 9	2019-								
firepower_ma	anagen	nent_c	enter_4	600_fi	rmware	!								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-	-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execute code interf sensitinform	ple vulnereb-based gement Firepower gement (and a could a coul	interface ver Center allow an anduct a pting (X a user of anagement input be anagement attacker these s by user of t ick a crassful explance attacker ary scri- ntext of access	e of SSS) of the ent e to of y the ent che afted oit cer to pt the	N/	'A		O-CIS-F 041119			
Improper Neutralizati on of Input	16-10-	-2019	3.5	Multiple vulnerabilities in the web-based management interface of				the web-based N/A					O-CIS-F 041119	
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')	Publish Date	CVSS	Cisco Mana (FMC authe attacl cross attacl web- interf vulne insuff user- web- interf could vulne persu interf link. A could execu- code interf sensi information	Firepove agement of could a conticated ker to consider the constant of the con	ver Center allow an I, remote induct a ipting (X it a user of anagement ese s are du alidation I input b anagement attacker these s by user of t ick a cra sful expl ne attack rary scri ontext of ccess wser-ba	es (SS) of the ent of y the ent of the oft ser to pt of the oft of the oft ser to pt of the oft of	Pato	;n	NCIIP	CID
firepower_m	anagement_ce	nter_2	1526 500_fi)					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wana Cisco Mana (FMC auther attack cross attack web-	ple vuln yeb-base gement gement could a enticated ker to co -site scri k against based m	d interfactory ver Center allow an I, remote induct a ipting (X t a user of	e of (SS) of the	N/A		0-CIS-F 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			insuff user-s web-l interf could vulne persu interf link. A could execu code s interf sensit inform	rabilities rabilities supplied based ma face. An a exploit of rabilities ading a success allow the arbitrin the corace or active, brownation.	ilidation input by anagementtacker these s by user of the ick a cra sful expl a attack ary scri ntext of ccess wser-ba	he of ter to pt the				
			1526		2017					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross- attack web-l interf vulne insuff user-s web-l interf could vulne persu interf link. A	ple vulne eb-based gement in Firepow gement in Could a enticated ker to con- site scri k against cased ma face. The rabilities ficient val supplied cased ma face. An a exploit in rabilities ading a in face to cli A success allow th	interface ver Center Illow an , remote nduct a pting (X a user of anagement input by anagement attacker these s by user of t ick a cra	e of SSS) of the ent e to of y the ent he afted oit	N/A		O-CIS-F 041119	
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	Pul	blish Date	CVSS	Description & CVE ID				Pa	atch	NCIIP	C ID
firepower_ar	1:	012		code interf sensit infort CVE I 1526	ite arbita in the co face or ac tive, bro mation. D: CVE-	ntext of ccess wser-ba	the				
mepower_up	рпа	1100_012			ple vuln	erabiliti	es in				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	mana Cisco Mana (FMC authe attack cross attack web-k interf vulne insuff user-web-k interf could vulne persu interf link. A could execu code interf sensit	eb-based gement Firepow gement Could a	interface ver Center allow and pring (X) a user of an agem se are dualidation input be an agem attacker these as by user of the actacker ary scription attacker ary scription attacker ary scription attacker ary scription attacker ary scription attacker ary scription attacker ary scription attacker	es (SS) of the ent e to of y the ent che afted loit ger to pt the	N/A		O-CIS-F 041119	
Improper Neutralizati	16-	10-2019	3.5	Multiple vulnerabilities in the web-based			N/A		O-CIS-F	IRE-	
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		escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
on of Input During Web Page Generation ('Cross-site Scripting')			mana Cisco Mana (FMC autho autho attac cross attac web- inter vulne insuf user- web- inter could vulne persu inter could execu code inter insuf	agement agement by Firepove agement c) could a centicated ker to co cesite scrip k against based m face. The cerabilitie ficient va supplied based m face. An a cerabilitie ading a face to cl A succes cerabilitie ading a face to cl ative arbit in the co face or a tive, bro mation. ID: CVE	interfactiver Center allow an I, remote nduct a ipting (X a user of an agementate attacker of the se ick a crassful explante attacker ary scripntext of access wser-bar	e of e (SS) of the ent e to of the ent che ent che fed loit cer to pt the			041119	
amp_7150_fi	rmware									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wana Cisco Mana (FMC) author attack	iple vuln veb-base gement Firepov gement C) could a enticated ker to co s-site scri k against based m	d interfac ver Center allow an l, remote nduct a ipting (X t a user o	e of (SS) of the	N/A		O-CIS-A 041119	_
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			vulne insuff user web-l interf could vulne persu interf link. A could execu code interf sensit inform	rabilities rabilities rabilities supplied based ma face. An a exploit of rabilities ading a of ace to clo ace to clo ace to clo ace to clo ace or accive, brownation. D: CVE-	s are dualidation input be anagement these is by user of the acrassing arry scripters of the attack for arry scripters of exess weer-ba	the of the oit the oit the oit the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multi the w mana Cisco Mana (FMC authe attack cross attack web-l interf vulne insuff user-s web-l interf could vulne persu interf		erabilition d interface ver Center llow an , remote nduct a pting (X a user of anagement input b anagement input b anagement ithese s by user of t ick a cra	e of (SS) of the ent e to of y the ent	N/A		O-CIS-A 041119	_
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
firepower_ap	opliance_8350	firmw	could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. CVE ID: CVE-2019-15269 are		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268	N/A	O-CIS-FIRE- 041119/944

Weakness	Publish Date	cvss	Description & CVE ID	Patch		NCIIPC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker execute arbitrary script code in the context of the interface or access sensitive, browser-based information. CVE ID: CVE-2019-15269	ne N/A		O-CIS-FIRE- 041119/945
firepower_ap	ppliance_8140	_firmw	are			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS)	N/A		O-CIS-FIRE- 041119/946
CV Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5	6-6 6-7	7-8	8-9 9-10

(CVSS)

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			web-linterf vulne insuff user-s web-linterf could vulne persu interf link. A could execu code i interf sensit inform CVE I		anagemose se s are due lidation input be anagemo attacker these s by user of t ick a cra sful expl ae attack ary scri ntext of ccess wser-ba	ent e to of y the ent the oft oft the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC) authe attack cross attack web-k interf vulne insuff user-s web-k interf could	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by					0-CIS-F 041119	
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	Pate	ch	NCIIP	C ID
			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 access sensitive, browser-based information. CVE ID: CVE-2019-				
			15269				
firepower_ap	pliance_7050_	firmw					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-	N/A		0-CIS-F 041119	
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	Pul	blish Date	cvss	D	escription	a & CVE II	D	Pat	ch	NCIIP	C ID
				1526	8						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterfi vulne insuffi user-sweb-linterfi could vulne persuinterfi link. A could execut code sinterfi sensiti informatical contractions attack web-linterfi could vulne persuinterfi link. A could execut code sinterfi sensiti informatical contractions attack web-linterfi could execut code sinterfi sensiti informatical contractions attack web-linterfi could execut code sinterfi sensiti informatical contractions attack web-linterficient web	ple vulne eb-base gement Firepow gement) could a nticated ker to co site scri k against based ma face. The rabilitie ficient va supplied based ma face. An a exploit rabilitie ading a face to cl A success allow th te arbitr in the co face or ac cive, brow mation. D: CVE- 9	tinterface ver Center Illow an , remote nduct a pting (X a user of anagement input be anagement input be are attack are are attack anagement input be are attack anagement input be are attack anagement input anagement input anageme	e of (SS) of the ent e to of y the ent he oft er to pt the	N/A		0-CIS-F 041119	
firepower_ap	plia	nce_826	60_firmv	vare							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	the w mana Cisco Mana (FMC authe	ple vulno eb-based gement Firepow gement) could a nticated ker to co	d interface ver Center llow an , remote	e of	N/A		0-CIS-F 041119	
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	D	escriptio	n & CVE I	D	P	atch	NCIIF	C ID
			attack web-l interf vulne insuff user-s web-l interf could vulne persu interf link. A could execu code interf sensit inform	ratic script against based marabilities ficient variabilities and a exploit based marabilities ading a face to classed allow that arbitration the continuity, brown ation. D: CVE-8	a user of anagements and anagements anagements attacker of these as by user of the attacker ary script and attacker are attacker and attacker are attacker attacker are attacker attacker attacker are attacker	e to of the ent e to of of y the ent che afted loit cer to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross attack web-l interf vulne insuff user-web-l interf could	ple vulnieb-base gement Firepow gement Could a enticated act to co-site scrit against based marabilitie ficient value assed marabilitie face. An act exploit arabilitie arabilitie arabilitie arabilitie arabilitie arabilitie arabilitie arabilitie	interfactiver Center Allow an I, remote and I (X) and I	e of (SS) of the ent e to n of y the ent	N/A		O-CIS-F 041119	
CV Scoring Scal	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 8	& CVE ID	Pato	h	NCIIP	C ID
			persuading a us interface to click link. A successful could allow the execute arbitrary code in the continterface or accessensitive, brows information. CVE ID: CVE-20, 15269	k a crafted all exploit attacker to by script eext of the eess ser-based				
firepower_ap	ppliance_8360_	firmw	are					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerathe web-based management into Cisco Firepower Management Ce (FMC) could allow authenticated, rattacker to conductorss-site script attack against a web-based man interface. These vulnerabilities a insufficient valid user-supplied in web-based man interface. An attacker to click persuading a us interface to click link. A successful could allow the execute arbitrary code in the continuerface or accessensitive, brows information.	terface of center ow an emote duct a sing (XSS) user of the agement agement eacker ese by er of the attacker to by script eext of the ess	N/A		0-CIS-F 041119	
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	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	C ID
			_	D : CVE- 8	-2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269		N/A		O-CIS-F 041119			
firepower_m	anagement_c	enter_fi	irmwa	re						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	3.5	A vulnerability in the web- based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to				N/A		O-CIS-F 041119	
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
Scripting')			conduct a cross-site scripting (XSS) attack against a user of the webbased management interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. 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 access sensitive, browser-based information. CVE ID: CVE-2019-15270		
500_series_fi	rmware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this	N/A	O-CIS-500 041119/955

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D		Pato	h	NCIIP	C ID
			persu interf malic subse specif page. could execu code affect acces based	rability lading a lace to cl lous link equently fic web i A succes allow th te arbita in the co ed inter s sensiti l informa D: CVE-	user of to ick a access a access a access a access a access a access accessful exponential accessful exponential accessful accessful exponential accessful exponential accessful accessful excessful	oloit er to pt the					
Citaria			1271	8							
Citrix	lalivary cant	collor f	irmwa	ro							
application_c	ienvery_conti	roner_n	_		1.	1 .					
Improper Authenticati on	21-10-2019	7.5	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway before 10.5 build 70.8, 11.x before 11.1 build 63.9, 12.0 before build 62.10, 12.1 before build 54.16, and 13.0 before build 41.28. An attacker with management-interface access can bypass authentication to obtain appliance administrative access. These products formerly used the NetScaler brand name. CVE ID: CVE-2019-					I/A		O-CIT-A 041119	
gateway_firm	iware										
Improper Authenticati	21-10-2019	7.5		sue was Applica			N	I/A		O-CIT-G 041119	
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	h	NCIIPC	ID
on			Controller (ADC) and Gateway before 10.5 build 70.8, 11.x before 11.1 build 63.9, 12.0 before build 62.10, 12.1 before build 54.16, and 13.0 before build 41.28. An attacker with management-interface access can bypass authentication to obtain appliance administrative access. These products formerly used the NetScaler brand name. CVE ID: CVE-2019- 18225				
netscaler_gat	teway_firmwaı	re					
Improper Authenticati on	21-10-2019	7.5	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway before 10.5 build 70.8, 11.x before 11.1 build 63.9, 12.0 before build 62.10, 12.1 before build 54.16, and 13.0 before build 41.28. An attacker with management-interface access can bypass authentication to obtain appliance administrative access. These products formerly used the NetScaler brand name. CVE ID: CVE-2019-18225	N/A		O-CIT-NE 041119/	
clonos							
CIUIIUS							
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	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
Session Fixation	24-10-2019	7.5	control remote full ac passw becau sessio	ol panel te attack ccess via vord req se there on mana	uests is no gement.	lows ain	N/A		0-CLO-0 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	4.3	(XSS) index contro remote arbitr HTMI paran	.php in (ol panel te attack ary web wia the neter. D: CVE-	bility in ClonOS V 19.09 al ers to in script o lang	lows iject	N/A		0-CL0-0 041119	
comtechefda	ta									
h8_heights_re	emote_gatewa	y_firm	ware							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	17-10-2019	3.5	Remo device HTMI Name field.	es allow Linjectio	vay 2.5.1 XSS and on via th ceName)	l e Site	N/A		O-COM- 041119	_
Scripting')			1766	7						
Debian										
debian_linux										
Out-of- bounds Write	28-10-2019	7.5	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to				https:// php.net/ hp?id=7/ https:// rt.f5.com /article/ 08500?u	bug.p 8599, suppo 1/csp K754	O-DEB- 041119	
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	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			buffer reservedata, possil execu	D : CVE-	e space CGI pro ning the cemote o	9	ource=f5 ort& _medium	;utm		
N/A	16-10-2019	2.6	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with a multi comp SE En attack intera other Succes vulne unaut cause service Java SEmbe vulne Java of typica sandk applie Java a that le	erability and SE Emponent: It promotes and and and and a sted code and a sted code a sted	nbedded acle Java Network rsions the sions the sions the sions the sions the sions at the sed attacked access where access to ava SE, J. Success to ava SE, J. Success to ava SE, J. Success the human aper elattacked acks of the sandbility the sions ability the sions ability the sions are single sides. This applies the sions are sandbility than Java Sir sandbility and Sir sandbility the sides are sandbility the sides are sandbility than Java Sir sandbility and Sir sa	s SE sting). The string	https://sty.netapj/advisorp-201910001/	p.com ry/nta	O-DEB-1 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
			interr Java s This v apply typica load a code (by an 3.0 Ba (Avail CVSS (CVSS N/UI:	omes fromet) and andbox for all year of a dministration in the content of the con	rely on for secuility doe deploymers, the only trusted install trator). A second contract of the contract of t	rity. es not nents, nat sted led CVSS . I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppo are af 7u23213; Ja 8u2221 vulne unaut with r Kerbe Java S Embe vulne Java S may s additi Succe vulne unaut critica access SE Em	rability in sect of Oractor of Oractor of Oractor of Oractor of Section 1, 8u221 oract	nbedded acle Java Kerbero rsions the re Java S , 11.0.4 nbedded alt to exp allows red attace access v omprom EE hile the as in Java dded, attace acks of t can resu access t r comple	I SE s). nat SE: and d: cloit cker via nise chis act chis clt in co ete ava	https://sty.netapy/advisorp-20191	p.com ry/nta	O-DEB- 041119	
			data.	Note: Th	is					

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			Java of typical sandhapplical	rability a leployme ally in clip loxed Jav cations of pplets (in cations of pplets) and candbox in the ploited by specifie to onent, ending the cation of th	ents, ents rur va Web S r sandb in Java S run le (e.g., c om the rely on t for secu ility can by using d l.g., throu vhich to the A Score 6 ty impact :N/AC:H :H/I:N/	nning Start oxed E 8), ode the rity. also APIs ugh a PIs8 cts).				
N/A	16-10-2019	5.8	SE prosection SE prosection SE (construction SE (construc	erability in oduct of componer or ted verefected and 13 it vulners unauthous via multiple of the cols to cols	Oracle Jat: Hotsparsions the Java Son Difficult ability denticated ability cathorized a subsectible data	ava bot). lat E: t to ed acks an t of a	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	O-DEB- 041119	
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	D	escriptior	ı & CVE II	D	Pato	:h	NCIIP	CID
			service Java S vulne Java d typical sandb applied Java a that le untru that continue internation Java sandb apply typical load a code (by an 3.0 Ba (Confi Availa Vecto (CVSS N/UI:	ce (partial E. Note: rability and leployment of the code ones from the	al DOS) of This applies to ents, dents run le (e.g., com the rely on the rely on the only trus le install strator). Le 4.8 ty and apacts). Le 'N/AC:HC:L/I:N/AC:HC	of to nning Start oxed EE 8), code the rity. es not nents, nat sted led CVSS I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Jav produ (comp Suppo are af 7u232 13; Ja 8u222 vulne unaut with r multip comp	erability in va SE Employers of Oractor of O	nbedded acle Java Network rsions the re Java S , 11.0.4 anbedded alt to exp allows ted attac access v	I SE king). hat SE: and d: bloit ker via	https://sty.netapgi /advisor p-20191 0001/	p.com y/nta	O-DEB- 041119	
			CE E~	nbedded	Success	cful				

Weakness	Publish Date	CVSS	D	escription	1 & CVE I	D	Pato	:h	NCIIP	CID
			attack vulne unaut cause service Java S Embe vulne Java d typica sandh applie Java a that le untru that c interregion Java s This was the expirate the Compweb s supple CVSS (Avail CVSS (CVSS N/UI:	as of this rability of thorized a partial ce (partial	can result ability to a le	alt in so of of of start oxed sE 8), sode the rity. also APIs ugh a PIs. 5.7 .				
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker			https:// ty.netap /advisor p-20191 0001/	p.com y/nta	O-DEB- 041119		
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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			multiple compose service Java Service Se	network ple proto romise Ja nbedded as of this rability of thorized a partia E, Java S edded. No rability a deployme ally in cli boxed Jav cations o applets (i oad and i asted cod omes fro net) and sted cod omes fro ome	cools to ava SE, J. Succes can resurability to denial al DOS) of the content of t	lava sful lt in so of of start oxed let 8), sode the rity. also APIs also APIs lgh a lf. 7.				
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u231, 8u221,			https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	O-DEB- 041119		
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	D	escription	& CVE I	D	Pato	h	NCIIP	CID
Weakness	Publish Date	CVSS	11.0.4 Emberoulner unaut with a multi comp SE En attack vulner unaut cause service Java SEmberoulner SEMBEROU	dand 13, added: 80 athenticate protocorrections of this expections of the cations	E Java SE allows access to access to ava SE, Java SE, Jav	cker via lava sful lit in of of sto nning Start oxed EE 8), code the rity. also APIs ugh a PIs. 1.7	Pato	:h	NCIIP	CID
			N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2983							
N/A	16-10-2019	4.3	Vulnerability in the Java SE product of Oracle Java			https://s		O-DEB-	DEBI-	
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	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			SE (co	omponer	nt: 2D).		/advisor	y/nta	041119	/969
			Supp	orted vei	rsions th	nat	p-20191	017-		
			are af	fected a	re Java S	SE:	0001/			
			11.0.4	and 13.	Difficul	t to				
			explo	it vulner	ability					
			allow	s unauth	enticate	ed				
			attacl	ker with	networl	K				
			acces	s via mu	ltiple					
			proto	cols to c	ompron	nise				
			Java S	E. Succe	ssful att	acks				
			of thi	s vulnera	ability ca	an				
			result	in unau	thorized	d				
			abilit	y to caus	e a part	ial				
			denia	l of servi	ice (part	tial				
			DOS)	of Java S	E. Note:	This				
			vulne	rability a	applies t	0				
			Java d	leploym	ents,					
			typica	ally in cli	ents rur	nning				
			sandb	oxed Jav	7a Web S	Start				
			appli	cations o	r sandb	oxed				
			Java a	ipplets (i	n Java S	E 8),				
			that l	oad and	run					
			untru	sted cod	e (e.g., c	ode				
			that c	omes fro	m the					
			interi	net) and	rely on t	the				
			Java s	andbox	for secu	rity.				
			This v	ulnerab/	ility can	also				
			be ex	ploited b	y using	APIs				
			in the	specifie	d					
			Comp	onent, e	.g., thro	ugh a				
			web s	ervice w	hich					
			suppl	ies data	to the A	PIs.				
			CVSS	3.0 Base	Score 3	.7				
			(Avai	lability ii	mpacts)					
			CVSS	Vector:						
			(CVSS:3.0/AV:N/AC:H/PR:							
			N/UI:N/S:U/C:N/I:N/A:L).							
			CVE ID : CVE-2019-2987							
			Vulnerability in the Java			https://s	securi	O-DEB-	DEBI-	
N/A	16-10-2019	4.3	SE, Java SE Embedded			ty.netap _]	p.com			
						/advisor	-	041119	7770	
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	0.10
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-0	0-7	7-8	8-9	9-10

(component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted	IPC ID
are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	
This vulnerability does not apply to Java deployments, typically in servers, that	
apply to Java deployments, typically in servers, that	
typically in servers, that	
load and run only trusted	
code (e.g., code installed	
by an administrator). CVSS	
3.0 Base Score 3.7	
(Availability impacts).	
CVSS Vector:	
(CVSS:3.0/AV:N/AC:H/PR:	
N/UI:N/S:U/C:N/I:N/A:L).	
CV Scoring Scale	

(CVSS)

Weakness	Publish Date	cvss	D	escription	1 & CVE I	D	Pato	:h	NCIIF	PC ID
			CVE I	D : CVE-	2019-2	988				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with a multi comp SE En attack vulne unaut cause service Java SEmber vulne Java at that le untru that cointern Java at apply typical load a code by an	erability in a SE Emponent: 2 ponent: 2 ponent	acle Java 2D). rsions the Java S, 11.0.4 abedded attacked attacke	a SE nat SE: and d: cloit cker via Java sful alt in to of sto nning Start coxed SE 8), code the rity. es not nents, nat sted led	https://ty.netap /advisor p-20191 0001/	p.com y/nta	O-DEB- 041119	
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
			(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2992		
Improper Input Validation	17-10-2019	9	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#\$((0xffffffff))" command. CVE ID: CVE-2019-14287	https://securi ty.netapp.com /advisory/nta p-20191017- 0003/, https://suppo rt.f5.com/csp /article/K537 46212?utm_s ource=f5supp ort&utm _medium=RSS , https://www. sudo.ws/alert s/minus_1_ui d.html	O-DEB-DEBI- 041119/972
Interpretati on Conflict	24-10-2019	5	Go before 1.12.11 and 1.3.x before 1.13.2 can panic upon an attempt to process network traffic containing an invalid DSA public key. There are several attack scenarios, such as traffic from a client to a server that verifies client certificates. CVE ID: CVE-2019-17596	https://githu b.com/golang /go/issues/3 4960, https://group s.google.com/ d/msg/golang - announce/IVE m7llp0w0/Vb afyRkgCgAJ	O-DEB-DEBI- 041119/973
Out-of- bounds Write	21-10-2019	7.5	cdf_read_property_info in cdf.c in file through 5.37 does not restrict the number of CDF_VECTOR elements, which allows a	N/A	O-DEB-DEBI- 041119/974

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			heap-based buffer overflow (4-byte out-of-bounds write).		
			CVE ID : CVE-2019- 18218		
Use After Free	24-10-2019	5	archive_read_format_rar_r ead_data in archive_read_support_for mat_rar.c in libarchive before 3.4.0 has a use-after-free in a certain ARCHIVE_FAILED situation, related to Ppmd7_DecodeSymbol.	N/A	O-DEB-DEBI- 041119/975
			CVE ID : CVE-2019- 18408		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments,	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	O-DEB-DEBI- 041119/976
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	Publi	ish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				applied Java and that let untrue that continued in the Company web so supplicated CVSS (Available CVSS (CVSS N/UI:	sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2962 Vulnerability in the Java SE, Java SE Embedded						
N/A	16-10	0-2019	4.3	SE, Ja produ (comp Concu versic are Ja 11.0.4 Embe Diffic vulne unaut with i multi comp SE En attack vulne unaut	•			https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	O-DEB- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2964							
			CVE I	D : CVE-	2019-2	964				
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to			https://sty.netapging.p-20191	p.com ry/nta	O-DEB- 041119		
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	D	escription	ո & CVE II	D	Pato	ch	NCIIP	CID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2973 Vulnerability in the Java SE Embedded							
N/A	16-10-2019	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to			https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	O-DEB- 041119		
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
			some of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L). CVE ID: CVE-2019-2975		
Dlink					1
dir-412_firm	ware				
Improper Authenticati on	16-10-2019	6.4	There are some web interfaces without authentication requirements on D-Link DIR-412 A1-1.14WW routers. An attacker can clear the router's log file via	N/A	0-DLI-DIR 041119/980
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 588	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			act=clear&logtype=sysact to log_clear.php, which could be used to erase attack traces. CVE ID : CVE-2019- 17512		
dir-866l_firm	ıware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	D-Link DIR-866L 1.03B04 devices allow XSS via HtmlResponseMessage in the device common gateway interface, leading to common injection. CVE ID: CVE-2019-17663	N/A	O-DLI-DIR 041119/981
eq-3					
homematic_c	ccu3_firmware				
Session Fixation	17-10-2019	4.9	eQ-3 HomeMatic CCU3 firmware 3.41.11 allows session fixation. An attacker can create session IDs and send them to the victim. After the victim logs in to the session, the attacker can use that session. The attacker could create SSH logins after a valid session and easily compromise the system. CVE ID: CVE-2019-15849	N/A	O-EQHOME- 041119/982
Improper Input Validation	17-10-2019	9	eQ-3 HomeMatic CCU3 firmware version 3.41.11 allows Remote Code Execution in the ReGa.runScript method. An authenticated attacker	N/A	O-EQHOME- 041119/983
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			and co	asily exe omprom n. D : CVE -	ise the	le				
			1585		2019-					
ccu2_firmwa	re									
Improper Control of Generation of Code ('Code Injection')	17-10-2019	9	A Remote Code Execution (RCE) issue in the addon CUx-Daemon 1.11a of the eQ-3 Homematic CCU-Firmware 2.35.16 until 2.45.6 allows remote authenticated attackers to execute system commands as root remotely via a simple HTTP request. CVE ID: CVE-2019-14423				N/A		CCU2- /984	
					2019-					
Information Exposure	17-10-2019	4				N/A		O-EQ0 041119		
			CVE I 1442	D : CVE- 4	2019-					
Fedoraproje	ct									
fedora										
Improper Input Validation	17-10-2019	9	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by				https://sty.netapy/advisorp-201910003/, https://str.f5.com	p.com ry/nta 017- suppo	0-FED-1 041119	
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
			invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#\$((0xffffffff))" command. CVE ID: CVE-2019-14287	/article/K537 46212?utm_s ource=f5supp ort&utm _medium=RSS , https://www. sudo.ws/alert s/minus_1_ui d.html	
hinet					
gpon_firmwa	re				
Improper Input Validation	17-10-2019	7.5	An ?invalid command? handler issue was discovered in HiNet GPON firmware < I040GWR190731. It allows an attacker to execute arbitrary command through port 3097. CVSS 3.0 Base score 10.0. CVSS vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:H/I:H/A:H) CVE ID: CVE-2019- 13411	2 h+ml	O-HIN-GPON- 041119/987
Information Exposure	17-10-2019	5	A service which is hosted on port 3097 in HiNet GPON firmware < I040GWR190731 allows an attacker to execute a specific command to read arbitrary files. CVSS 3.0 Base score 9.3. CVSS vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:H/I:N/A:L). CVE ID: CVE-2019-13412		O-HIN-GPON- 041119/988
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6 6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
Improper Authenticati on	17-10-2019	7.5	HiNet GPON firmware version < I040GWR190731 allows an attacker login to device without any authentication. CVE ID : CVE-2019- 15064	https://tvn.tw cert.org.tw/ta iwanvn/TVN- 201908007, https://www. twcert.org.tw /en/cp-128- 3015-170fe- 2.html	O-HIN-GPON- 041119/989		
Information Exposure	17-10-2019	5	A service which is hosted on port 6998 in HiNet GPON firmware < I040GWR190731 allows an attacker to execute a specific command to read arbitrary files. CVSS 3.0 Base score 9.3. CVSS vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:H/I:N/A:L). CVE ID: CVE-2019-15065	https://tvn.tw cert.org.tw/ta iwanvn/TVN- 201908011, https://www. twcert.org.tw /en/cp-128- 3016-b0e90- 2.html	O-HIN-GPON- 041119/990		
Improper Input Validation	17-10-2019	10	An ?invalid command? handler issue was discovered in HiNet GPON firmware < 1040GWR190731. It allows an attacker to execute arbitrary command through port 6998. CVSS 3.0 Base score 10.0. CVSS vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:H/I:H/A:H). CVE ID: CVE-2019-	https://tvn.tw cert.org.tw/ta iwanvn/TVN- 201908012, https://www. twcert.org.tw /en/cp-128- 3017-fd6bc- 2.html	O-HIN-GPON- 041119/991		
Honeywell			15066				
ip-ak2_firmw	vare						
Missing	25-10-2019	5	In IP-AK2 Access Control	N/A O-HON-IP-			
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	D	escriptio	n & CVE I	D		Patc	h	NCIIP	C ID
Authenticati on for Critical Function			Panel Version 1.04.07 and prior, the integrated web server of the affected devices could allow remote attackers to obtain web configuration data, which can be accessed without authentication over the network. CVE ID: CVE-2019-13525							041119	/992
			1352	5							
НР			15025								
futuresmart_	.3										
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				I/A		O-HP-F 041119		
futuresmart_	4		0,2,	2.0.2							
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				O-HP-F 041119			
inea											
me-rtu_firmv Incorrect Default Permissions	vare 28-10-2019	4	on Mi RTU (An issue was discovered on Mitsubishi Electric ME- RTU devices through 2.02 and INEA ME-RTU devices			N	I/A		O-INE-N 041119	
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	D	escription	ո & CVE I	D	Pato	:h	NCIIP	C ID
			reada /usr/ gs.xm on the an att sensit settin usern and o data o perm	smartrtud configure file systacker to tive configures such a ther send ther send ther to in the to in the to in the to in the to the total t	u/init/so iration f tem allo read iguratio as assword sitive R' secure signmen	ettin file ows on Is,				
Use of Hard-coded Credentials	28-10-2019	7.5	on Mi RTU of and II throu SSH k to gai acces encry due to regen instal firmw word priva /etc/ ey, an /etc/ y files availa web s	ssh/ssh_s that are able from sites. D: CVE-	Electrice hrough RTU de lard-coc w an atta norised lose a on the ex not be n initial with ates. In devices in host_rsa host_ec host_ds publicl n the ver	e ME- 2.02 vices led acker e RTU eing other use a_key dsa_k a_ke y	N/A		O-INE-N 041119	
Information	28-10-2019	5	An issue was discovered				N/A		O-INE-N	ИЕ-R-
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	e CVSS	D	escriptio	n & CVE I	D	Pate	h	NCIIP	CID
Exposure			RTU of and II throu unaut config vulne attack smart file (v such a passw sensit	tsubishidevices to NEA MEand and the substitution as usern words, and tive RTU.	hrough RTU de An ted remo allows a ownload onfigura ntains d ames, nd other (data).	2.02 vices ote ad n the ation ata			041119	/997
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	28-10-2019	3.5	on Mi RTU (and II throu store (XSS) an att malic into t exam vulne Serial in the	sue was tsubishidevices to NEA ME gh 3.0. And crosses wulnerated acker to ious codhe applicable to Initial Me index.p	Electrice hrough -RTU de A number site script bilities a inject de direct cation. A t variable stored of the page	e ME- 2.02 vices er of ot allow ly An le KSS is	N/A		O-INE-N 041119	
Insufficientl y Protected Credentials	28-10-2019	5	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Stored cleartext passwords could allow an unauthenticated attacker to obtain configured username and				N/A		O-INE-N 041119	
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	D	escription	n & CVE I	D		Pato	h	NCIIP	C ID
			weak mana An un can of passw gain a follow service Provi service CVE I	on the RTU due to the weak credentials management on the RTU. An unauthenticated user can obtain the exposed password credentials to gain access to the following services: DDNS service, Mobile Network Provider, and OpenVPN service. CVE ID: CVE-2019- 14929 An issue was discovered on Mitsubishi Electric ME-							
Use of Hard- coded Credentials	28-10-2019	10	14929 An issue was discovered				N/	'A		O-INE-N 041119	
Improper Neutralizati on of Special Elements used in an	28-10-2019	10	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An				N/	'A		O-INE-N 041119	
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
OS Command ('OS Command Injection')			unauthenticated remote OS Command Injection vulnerability allows an attacker to execute arbitrary commands on the RTU due to the passing of unsafe user supplied data to the RTU's system shell. Functionality in mobile.php provides users with the ability to ping sites or IP addresses via Mobile Connection Test. When the Mobile Connection Test is submitted, action.php is called to execute the test. An attacker can use a shell command separator (;) in the host variable to execute operating system commands upon submitting the test data.		
			CVE ID : CVE-2019- 14931		
Linux					
linux_kernel					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-10-2019	7.2	IBM DB2 High Performance Unload load for LUW 6.1 and 6.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 165481.	https://suppo rtcontent.ibm. com/support/ pages/node/1 073236	O-LIN-LINU- 041119/1002

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			CVE I	D : CVE-	2019-4	523				
Improper Input Validation	18-10-2019	9	certain than (setuse flags to prima second platform possible change initial group CVE I	rtl_p2p_noa_ie in drivers/net/wireless/real tek/rtlwifi/ps.c in the					0-LIN-I 041119	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-10-2019	8.3	cve ID: cve-2019-15901 rtl_p2p_noa_ie in drivers/net/wireless/real tek/rtlwifi/ps.c in the Linux kernel through 5.3.6 lacks a certain upper-bound check, leading to a buffer overflow. cve ID: cve-2019-17666				N/A		O-LIN-I 041119	
Use After Free	18-10-2019	6.8	Linux kernel through 5.3.6 lacks a certain upperbound check, leading to a buffer overflow. CVE ID: CVE-2019-				N/A		0-LIN-I 041119	
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	Pul	blish Date	cvss	D	escriptio	n & CVE I	D		Pate	ch	NCIIF	PC ID	
					sclosed. D : CVE - 7	2019-							
Missing Release of Resource after Effective Lifetime	18-	10-2019	7.2	5.3.4, usage fib6_r function suppression net/ip when FIB_L can be attack memory ca7a0 CVE I	e Linux k a refere e error in rule_supplion in the ression fov6/fib6 handlin OOKUP_ e exploit ker to coory, aka 03c4175 D: CVE- 8	nce count the press() e fib6 eature of the NOREF and by a rrupt CID-3.	f flag,	N/A			O-LIN-LINU- 041119/1000		
Use After Free	24-	10-2019	5	ead_d archiv mat_r befor after- ARCH situat	archive_read_format_rar_r ead_data in archive_read_support_for mat_rar.c in libarchive before 3.4.0 has a use- after-free in a certain ARCHIVE_FAILED situation, related to Ppmd7_DecodeSymbol. CVE ID : CVE-2019-						0-LIN-I 041119		
mi													
millet_router	_3g_	firmwa	re				7	ı					
Improper Input Validation	23-	10-2019	7.5	on Xia devic stable tar.gz uploa uses t	An issue was discovered on Xiaomi Mi WiFi R3G devices before 2.28.23-stable. The backup file is in tar.gz format. After uploading, the application uses the tar zxf command to decompress, so one can			N/A			O-MI-MILL- 041119/1008		
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	3-4	4-5	5-6		5-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID Patch						NCIIP	C ID
			control the contents of the files in the decompressed directory. In addition, the application's sh script for testing upload and download speeds reads a URL list from /tmp/speedtest_urls.xml, and there is a command injection vulnerability, as demonstrated by api/xqnetdetect/netspeed. CVE ID: CVE-2019-18370 An issue was discovered							
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	5	18370				N/A		O-MI-M 041119	
Microsoft										
windows										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-10-2019	7.2	Perfo for LU vulne overfi impro	DB2 High rmance JW 6.1 a rable to low, cau per boun could a	Unload Ind 6.5 is a buffer sed by ands che	s cking	https:// rtcontencom/sup pages/n 073236	it.ibm. pport/	0-MIC-\ 041119	
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	D	escriptio	n & CVE I	D	Patc	h	NCIIP	CID
			arbitr syster privil 1654	attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 165481. CVE ID: CVE-2019-4523						
Improper Input Validation	17-10-2019	6.6	12.0 c Deep vulne file de may l impac requi only v affect	D : CVE-	end Mic Agent a an arbit ack, whice vailabilit OS acces ase note s agents	ro are crary ch ty ss is that	N/A		O-MIC-V 041119	
Out-of- bounds Write	25-10-2019	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 processing of Javascript in the HTML2PDF plugin. 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 object. An attacker can leverage this vulnerability			N/A		O-MIC-\ 041119		
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
			to execute code in the context of the current process. Was ZDI-CAN-8692. CVE ID: CVE-2019-17139		
Untrusted Search Path	24-10-2019	6.9	A DLL side loading vulnerability in the Windows Service in TeamViewer versions up to 11.0.133222 (fixed in 11.0.214397), 12.0.181268 (fixed in 12.0.214399), 13.2.36215 (fixed in 13.2.36216), and 14.6.4835 (fixed in 14.7.1965) on Windows could allow an attacker to perform code execution on a target system via a service restart where the DLL was previously installed with administrative privileges. Exploitation requires that an attacker be able to create a new file in the TeamViewer application directory; directory permissions restrict that by default. CVE ID: CVE-2019-18196	https://comm unity.teamvie wer.com/t5/A nnouncement s/Security- bulletin-CVE- 2019- 18196/td- p/74564	O-MIC-WIND- 041119/1013
Improper Restriction of Operations within the Bounds of a Memory	23-10-2019	4.6	When executing VideoLAN VLC media player 3.0.8 with libqt on Windows, Data from a Faulting Address controls Code Flow starting at libqt_plugin!vlc_entry_lice	N/A	O-MIC-WIND- 041119/1014
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
Buffer			nse_3_0_0f+0x000000000 03b9aba. CVE ID : CVE-2019-		
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8064	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1015
Incorrect Permission Assignment for Critical Resource	17-10-2019	7.5	Adobe Download Manager versions 2.0.0.363 have an insecure file permissions vulnerability. Successful exploitation could lead to privilege escalation. CVE ID: CVE-2019-8071	https://helpx. adobe.com/se curity/produc ts/adm/apsb 19-51.html	O-MIC-WIND- 041119/1016
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a cross-site scripting vulnerability. Successful exploitation could lead to information	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1017

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			disclosure.		
			CVE ID : CVE-2019-8160		
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1018
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a race condition vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8162	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1019
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1020

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have an out-of- bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8163		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8164	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1021
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8165	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1022
Improper	17-10-2019	6.8	Adobe Acrobat and Reader	https://helpx.	O-MIC-WIND-
CV Scoring Sco (CVSS)	ale 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
Restriction of Operations within the Bounds of a Memory Buffer			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a buffer overrun vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8166	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/1023
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8167	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1024
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	0-MIC-WIND- 041119/1025
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	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
			could disclo	essful explead to be sure . D: CVE-	informa	tion				
Incorrect Type Conversion or Cast	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8169			https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.			https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-V 041119		
Out-of- bounds Write	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148			0040	https:///adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119	
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
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of- bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8171		
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8172	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1029
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1030

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Р	atch	NCIIF	C ID
			CVE I	D : CVE	2019-8	173				
NULL Pointer Dereference	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8174				adobe curity ts/acr	//helpx. .com/se /produc obat/ap 49.html	O-MIC-' 041119	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.				adobe curity ts/acr	//helpx. .com/se /produc obat/ap 49.html	O-MIC-1 041119	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and			adobe curity ts/acr	//helpx. .com/se /produc obat/ap 49.html	O-MIC-\ 041119		
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	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8176		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8177	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1034
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8178	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1035
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,	https://helpx. adobe.com/se curity/produc	O-MIC-WIND- 041119/1036

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8179	ts/acrobat/ap sb19-49.html	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8180	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1037
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1038
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
			code execution .		
			CVE ID : CVE-2019-8181		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1039
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	9.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8183	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1040
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1041

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have an out-of- bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8184		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8185	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1042
Out-of- bounds Write	17-10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8186	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1043
Use After	17-10-2019	4.3	Adobe Acrobat and Reader	https://helpx.	O-MIC-WIND-
CV Scoring Sco (CVSS)	ale 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			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8187	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/1044
Use After Free	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8188	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1045
Out-of- bounds Read	17-10-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	0-MIC-WIND- 041119/1046
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	Pul	blish Date	CVSS	C	escriptio	n & CVE I	ID	Pato	h	NCIIP	CID
				could discle	essful explessful expless explored expless exp	informa	tion				
				CVE	ID : CVE	·2019-8	8189				
Out-of- bounds Read	17-	10-2019	4.3	version and example and example and example 2015 earlies boun Succession discless	dobe Acrobat and Reader ersions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bunds read vulnerability. Excessful exploitation ould lead to information sclosure.			https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119	
				CVE 1	ID : CVE	2019-8	3190				
Out-of- bounds Write	17-	10-2019	6.8	version and explored arbits	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8191		https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119		
Use After Free	17-	10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148		versions , 2019.012.20040 and earlier, 2017.011.30148 and		https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119	
CV Scoring Sca (CVSS)	ale	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
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8192		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8193	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1050
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1051

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	C ID
			CVE I	D : CVE-	2019-8	194				
NULL Pointer Dereference	17-10-2019	10	and e. 2017. earlie and e. 2015. earlie point vulne explo arbitr	versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8195 Adobe Acrobat and Reader				helpx. om/se oroduc oat/ap .html	O-MIC-\ 041119	
NULL Pointer Dereference	17-10-2019	10	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and			https://adobe.co curity/p ts/acrob sb19-49	om/se oroduc oat/ap	O-MIC-\ 041119		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html			O-MIC-\ 041119	
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	NCIIPC ID
			earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8197		
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8198	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1055
Out-of- bounds Write	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8199	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1056
Incorrect Type Conversion	17-10-2019	7.5	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier,	https://helpx. adobe.com/se curity/produc	O-MIC-WIND- 041119/1057

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
or Cast			2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8200	ts/acrobat/ap sb19-49.html	
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8201	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1058
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1059
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
			disclosure.		
			CVE ID : CVE-2019-8202		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1060
Out-of- bounds Read	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8204	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1061
NULL Pointer Dereference	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1062

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description 8	& CVE ID	Patc	h	NCIIP	CID
			earlier, and 2015.006.30503 earlier have an a pointer derefere vulnerability. Su exploitation cou arbitrary code e CVE ID : CVE-20					
Out-of- bounds Write	17-10-2019	7.5	Adobe Acrobat a versions, 2019. and earlier, 2017.011.30148 earlier, 2017.01 and earlier, 2015.006.30503 earlier, and 2015.006.30503 earlier have an abounds write vulnerability. Su exploitation cou arbitrary code earlier code	8 and 1.30148 3 and out-of- accessful ald lead to execution.	https://kadobe.co curity/pr ts/acrob sb19-49.	m/se roduc at/ap	O-MIC-V 041119	
Out-of- bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8207		https://kadobe.co curity/pr ts/acrob sb19-49.	m/se roduc at/ap	O-MIC-V 041119	
Use After	17-10-2019	6.8	Adobe Acrobat	and Reader	https://l	nelpx.	O-MIC-V	WIND-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 621	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
Free			versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8208	adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	041119/1065	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8209	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1066	
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	0-MIC-WIND-	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			could code	essful explead to a lead t	arbitrary n .	У				
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8211 Adobe Acrobat and Reader			https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119		
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148		https://badobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119			
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148			versions, 2019.012.20040 adobe.c and earlier, curity/ 2017.011.30148 and ts/acro		om/se roduc at/ap	O-MIC-V 041119	
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
			and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8213		
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1071
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1072

Weakness	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				CVE I	D : CVE-	2019-8	215				
Out-of- bounds Read	17-	10-2019	5	version and e 2017, earlie 2015, earlie bound Succe could disclo		9.012.2 .48 and 011.301 .03 and n out-of vulnerate coloitatio	48 classification	https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	0-MIC-V 041119	
Use After Free	17-	10-2019	6.8	disclosure . CVE ID : CVE-2019-8216 Adobe Acrobat and Reader versions , 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID : CVE-2019-8217				https://i adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	0-MIC-V 041119	
Out-of- bounds Read	17-	10-2019	5	CVE ID: CVE-2019-8217 Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and				https://adobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119	
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
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8218		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8219	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1076
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8220	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1077
Use After Free	17-10-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier,	https://helpx. adobe.com/se curity/produc	O-MIC-WIND- 041119/1078

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish D	ate	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
				earlie and e 2015 earlie 2015 earlie free v Succe could code	on 11.301 or, 2017. arlier, on 6.305 or, and on 6.305 or have a rulnerab on ssful exp lead to executio D: CVE-	011.301 003 and 003 and n use affility. oloitatio arbitrary	ter n	ts/acrob sb19-49			
Out-of- bounds Read	17-10-20)19	5	version and e 2017 earlie 2015 earlie bound Succession disclared	sure .	9.012.2 48 and 011.301 603 and n out-of vulnerate coloritatio	48 - oility. n tion	https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-V 041119	
Use After Free	17-10-20)19	6.8	could lead to information disclosure. CVE ID: CVE-2019-8222 Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary				https://ladobe.co curity/p ts/acrob sb19-49	om/se roduc at/ap	O-MIC-\ 041119	
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
			code execution .		
			CVE ID : CVE-2019-8223		
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1081
Use After Free	17-10-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and earlier, and 2015.006.30503 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8225	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1082
Information Exposure	17-10-2019	5	Adobe Acrobat and Reader versions, 2019.012.20040 and earlier, 2017.011.30148 and earlier, 2017.011.30148 and earlier, 2015.006.30503 and	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb19-49.html	O-MIC-WIND- 041119/1083

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have an incomplete implementation of security mechanism vulnerability. Successful exploitation could lead to information disclosure.		
			CVE ID : CVE-2019-8226		
Improper Privilege Managemen t	23-10-2019	7.5	Creative Cloud Desktop Application version 4.6.1 and earlier versions have Security Bypass vulnerability. Successful exploitation could lead to Privilege Escalation in the context of the current user.	N/A	O-MIC-WIND- 041119/1084
			CVE ID: CVE-2019-8236		
Inadequate Encryption Strength	23-10-2019	10	Adobe Acrobat and Reader versions 2019.012.20034 and earlier; 2019.012.20035 and earlier versions; 2017.011.30142 and earlier versions; 2017.011.30143 and earlier versions; 2015.006.30497 and earlier versions; 2015.006.30498 and earlier versions have an Insufficiently Robust Encryption vulnerability. Successful exploitation could lead to Security feature bypass in the context of the current user.	N/A	O-MIC-WIND- 041119/1085

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2019-8237		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier; 2019.010.20099 and earlier versions; 2017.011.30140 and earlier version; 2017.011.30138 and earlier version; 2015.006.30495 and earlier versions; 2015.006.30493 and earlier versions have a Path Traversal vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. CVE ID: CVE-2019-8238	N/A	O-MIC-WIND- 041119/1086
Improper Input Validation	21-10-2019	5.1	Trend Micro Anti-Threat Toolkit (ATTK) versions 1.62.0.1218 and below have a vulnerability that may allow an attacker to place malicious files in the same directory, potentially leading to arbitrary remote code execution (RCE) when executed. CVE ID: CVE-2019-9491	N/A	O-MIC-WIND- 041119/1087
Mitsubishiel	ectric				
smartrtu_firi	mware				
Incorrect Default Permissions	28-10-2019	4	An issue was discovered on Mitsubishi Electric ME- RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A world-	N/A	O-MIT-SMAR- 041119/1088
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	D	escription	ո & CVE I	D	Pato	:h	NCIIP	C ID
			gs.xm on the an att sensit settin usern and o data o perm	smartrtual configue file systacker to tive confugs such a ther send due to in ission as	ration factor allowed terms al	file ows on ds, ΓU				
Use of Hard- coded Credentials	28-10-2019	7.5	on Mi RTU of and II throu SSH k to gai acces encry due to regen instal firmw word priva /etc/ ey, an /etc/ y files availa web s	ssh/ssh_s that are able from sites.	Electrice hrough RTU de lard-cook w an atta norised lose a on the ex not be on initial with ates. In devices in host_rsa host_ec host_ds publicl in the ver	e ME- 2.02 vices led acker e RTU eing other use a_key dsa_k a_ke y	N/A		O-MIT-9 041119	
Information Exposure	28-10-2019	5		sue was (itsubishi			N/A		0-MIT-9	
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	S Description & CVE ID		D	Pat	tch	NCIIP	CID	
			and II throu unaut config vulne attack smart file (v such a passv sensit		RTU de an downlo allows a wnload onfigura anes, and other data).	ote ad n the ation ata				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	28-10-2019	3.5	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A number of stored cross-site script (XSS) vulnerabilities allow an attacker to inject malicious code directly into the application. An example input variable vulnerable to stored XSS is SerialInitialModemString in the index.php page. CVE ID: CVE-2019-14928				N/A		O-MIT-9	
Insufficientl y Protected Credentials	28-10-2019	5	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Stored cleartext passwords could allow an unauthenticated attacker to obtain configured username and password combinations				N/A		O-MIT-9 041119	
CV Scoring Scal	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	D	Description & CVE ID				Pato	h	NCIIP	CID
				weak mana An ur can o passv gain a follov service Province CVE I								
Use of Hard- coded Credentials	28-	10-2019	10	on Market and I through the RTU of and I through the accounts a escala with a passive entries the R	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Undocumented hard-coded user passwords for root, ineaadmin, mitsadmin, and maint could allow an attacker to gain unauthorised access to the RTU. (Also, the accounts ineaadmin and mitsadmin are able to escalate privileges to root without supplying a password due to insecure entries in /etc/sudoers on the RTU.) CVE ID: CVE-2019-				/A		O-MIT-9	
Improper Neutralizati on of Special Elements used in an OS	28-	10-2019	10	on M RTU (and I throu	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote						O-MIT-: 041119	
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	De	escription	& CVE I	D	Pa	tch	NCIIF	CID
Command ('OS Command Injection')			OS Command Injection vulnerability allows an attacker to execute arbitrary commands on the RTU due to the passing of unsafe user supplied data to the RTU's system shell. Functionality in mobile.php provides users with the ability to ping sites or IP addresses via Mobile Connection Test. When the Mobile Connection Test is submitted, action.php is called to execute the test. An attacker can use a shell command separator (;) in the host variable to execute operating system commands upon submitting the test data. CVE ID: CVE-2019- 14931							
Netapp										
clustered_da	ta_ontap									
Improper Input Validation	25-10-2019	5	Clustered Data ONTAP versions 9.2 through 9.6 are susceptible to a vulnerability which allows an attacker to use l2ping to cause a Denial of Service (DoS). CVE ID: CVE-2019-5508				N/A		O-NET- 041119	
opengroup										
unix										
Buffer Copy without Checking	22-10-2019	7.2	IBM DB2 High Performance Unload load for LUW 6.1 and 6.5 is				rtconte	/suppo ent.ibm. upport/	0-0PE- 041119	
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 Dat	e CVSS	D	escriptio	n & CVE I	D	Pato	ch	NCIIP	C ID
Size of Input ('Classic Buffer Overflow')			overfl impro which attack arbitr system privil 1654	rable to low, cau oper bou a could a cer to ex ary code m with reges. IBI 81. D: CVE-	sed by Inds che Ilow a lo ecute on the oot M X-Fore	cking ocal ce ID:	pages/n 073236	ode/1		
Opensuse										
leap										
Improper Input Validation	17-10-2019	9	attack Runas can by black modu incors invok crafte exam bypas config loggin \#\$((comm	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#\$((0xffffffff))" command.				securi p.com ry/nta .017- suppo n/csp /K537 itm_s 5 supp p;utm n=RSS www. /alert :_1_ui	O-OPE-1 041119	
Oracle										
solaris			171 -	makil'i	:	ma al -				
N/A	16-10-2019	4.4	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows low privileged				N/A		0-0RA- 041119	
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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			infras Oracle comp Solari vulne Solari signifi additi Succe vulne unaut insert some access unaut to a si Solari unaut cause service Oracle Base S (Confi and A CVSS (CVSS L/UI:	ker with structure e Solaris romise (is. While rability is, attack icantly it ional properties of Oracl sible data thorized to or delet thorized a partial is access thorized a partial e Solaris Score 5.3 identiality vailability Vector: 5:3.0/AV N/S:C/C D: CVE-	e where sexecuted oracle is in Oracle is in Oracle in Or	cle class cl				
N/A	16-10-2019	1.2	Solari Systen LDAP suppo affect explo allow attack infras Oracle	erability is produ ms (com Library orted ver ed is 11. it vulner s high pr ker with structure e Solaris romise (ct of Ora ponent:). The rsion tha Difficul rability rivileged logon to where execute	at is t to I	N/A		O-ORA- 041119	
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	D	escription	n & CVE I	D	Patc	:h	NCIIP	C ID
			require from a the attack vulne unaut cause service (Avail CVSS (CVSS H/UI:	is. Succestre huma a person tacker. So sof this rability of thorized a partial e Solaris Score 1.8 lability in Vector: S:3.0/AV R/S:U/OD: CVE-	n intera n other the Successfican resu ability the al denial al DOS) s. CVSS 3 mpacts)	ction han ful filt in fo of of .0 (/PR: A:L).				
N/A	16-10-2019	4.6	Vulne Solari System XScre support affect explo allow attack infrast Orack comp Solari vulne Solari signifi additi Succe vulne takeo CVSS (Confi and A	erability is productions (combet seed is 11. itable vurs is low private with extructure is. While rability is, attack icantly it is, attack icantly in itable ver of Ora. Base identiality ver of Ora. Was is a seed identiality of oral productions.	in the Oract of Oract of Oract of Oract of Oract of Oract of Oracle of the oracle of the oducts. acks of the can result of Score 8 of the of Oracle of Orac	racle acle at is lity the es to cle chis alt in laris.	N/A		0-0RA-3 041119	
			(CVSS	S:3.0/AV	:L/AC:L	/PR:				

Weakness	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
				L/UI:	N/S:C/C	:H/I:H/	A:H).				
				CVE I	D : CVE-	2019-3	010				
N/A	16-	10-2019	3.3	Solari Systems service daem versice 11. Di vulne privil logon where execu Oracl attack vulne unaut insert some acces unaut cause service Oracl Base S and A CVSS (CVSS L/UI:	is produms (communices & leg ons). The constant is ifficult to rability eged attention of Oracle of Oracle of Oracle of Oracle is ible date thorized a partial ce (partice Solaris Score 3.0 vailability Vector: 5:3.0/AV N/S:U/O	e suppo s affecte o exploit allows lo acker w nfrastru Solaris omprom s. Succes can resu update, te access	rted d is to ith cture ise sful dit in sto of of of -() rity cts).	N/A		0-0RA- 041119	
Redhat											
enterprise_li	nux_	desktop									
N/A		10-2019	2.6	SE, Ja produ (com) Suppo	va SE En act of Or ponent: orted ve	in the Ja nbedded acle Java Networl rsions th	l n SE king). nat	https:// ty.netar /adviso p-2019 0001/	p.com ry/nta	O-RED- 041119	
CV Scoring Sca	ile	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that Ioad and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:R/S:U/C:N/I:N/A:L).	Weakness	Publish Date	cvss	Descripti	on & CVE I	D	Pato	h	NCIIP	CID
8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				7u231, 8u22	21, 11.0.4	and				
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				13; Java SE E	Embedded	d:				
unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				8u221. Diffic	cult to exp	oloit				
with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS: 3.0/AV:N/AC:H/PR:				vulnerability	allows					
multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS'3.0/AV:N/AC:H/PR:				-		cker				
compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				with networ	k access v	<i>r</i> ia				
compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				multiple pro	tocols to					
SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				• •		lava				
interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:				-	-					
interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:				attacks requ	ire huma	n				
other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:				_						
vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					-					
vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				Successful a	ttacks of t	his				
unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-						
service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					-					
Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-						
Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS: 3.0/AV:N/AC:H/PR:				7-	-	01				
vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-		10				
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				= -						
applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						_				
Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					•	E 8J,				
that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						,				
internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:						code				
Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				-	_					
apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				*		-				
typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:					_					
load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:										
code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				typically in s	ervers, th	nat				
by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				load and run	only tru	sted				
3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				code (e.g., co	de install	led				
(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				by an admin	istrator).	CVSS				
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:				3.0 Base Sco	re 3.1					
(CVSS:3.0/AV:N/AC:H/PR:				(Availability	impacts)					
				CVSS Vector	:					
N/UI:R/S:U/C:N/I:N/A:L).				(CVSS:3.0/A	V:N/AC:H	I/PR:				
				N/UI:R/S:U/	'C:N/I:N/	A:L).				
CV Scoring Scale						·				

(CVSS)

Weakness	Publish Date	cvss	Description 8	& CVE ID		Pato	h	NCIIP	C ID
			CVE ID : CVE-2	019-2945	5				
N/A	16-10-2019	4.3	Vulnerability in SE, Java SE Embroduct of Orace (component: Ke Supported vers are affected are 7u231, 8u221, 13; Java SE Embroduct of Successful attack with network a Kerberos to con Java SE, Java SE Embedded. Who vulnerability is Java SE Embedded. Who vulnerability is Java SE Embedded and significant additional productional pro	bedded cle Java SE erberos). cions that glava SE: 11.0.4 and bedded: to exploid lows d attacker ccess via mpromise ile the in Java SE ded, attack ly impact lucts. cks of this in result in ccess to complete ra SE, Java accessible soplies to ints, ints runnir a Web Star sandboxe glava SE 8 in (e.g., code in the ely on the ely on the or security ity can als a using API	d it re. E, ks in ng rt ed 3), e	https://s ty.netap /advisor p-20191 0001/	o.com y/nta	O-RED- 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4	4-5 5	5-6	6-7	7-8	8-9	9-10

Weakness	Pub	olish Date	CVSS	C	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				web s supp CVSS (Conf CVSS (CVSS N/UI CVE I	service values data 3.0 Base fidential Vector: S:3.0/AV :N/S:C/O	which to the A e Score 6 ity impa ':N/AC:H C:H/I:N/	PIs. 5.8 cts). I/PR: A:N).				
N/A		10-2019	4.3	SE, Ja production Supplare at 7u23 13; Ja 8u22 vulne unau with multicomp SE Errattack unau cause service Java SE Embervulne Jav	erability va SE Er uct of Or ponent: orted ve ffected a 1, 8u222 va SE Er 1. Difficit erability thentica network ple prot oromise erability thorized e a partia ce (parti SE, Java S edded. N erability deploym ally in cl poxed Ja cations o applets (oad and asted cod comes fr net) and	nbedded acle Java Network rsions the re Java St., 11.0.4 mbedded alt to expand allows ted attack access to cools to Java SE, ability to all denial all DOS) SE ote: This applies the ents, ients run de (e.g., com the com the	a SE king). hat SE: and d: bloit cker via Java sful dit in so of of to nning Start oxed SE 8), code	https://sty.netapj /advisor p-20191 0001/	p.com y/nta	O-RED-1 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				This very be explicated by the explication of the composition of the c	vulnerab ploited b specifie conent, e cervice w ies data 3.0 Base lability i Vector: 5:3.0/AV N/S:U/O	g., thro	also APIs ugh a PIs. .7 I/PR: A:L).				
N/A	16-10-20	019	4.3	Vulnes SE, Jar produ (comp Suppor are aff 7u23 13; Ja 8u22 vulnes unaut with a multi comp SE Emattack vulnes unaut cause service Java SE Ember vulnes	erability va SE En oct of Or ponent: ported ve fected a 1, 8u221 va SE Er 1. Difficurability chentical a partial a partial e (partice) feed ded. Norized a partial e (partice) ded. Norized Java Sections o (partice) ded.	in the Janbedded acle Java JAXP). rsions the re Java Standard attack access to cools to lava SE, judgment al DOS) SE ote: This applies to access the cools to lava SE, judgment al DOS) SE ote: This applies to access the cools to lava SE, judgment al DOS) SE ote: This applies to access the cools to lava SE, judgment al DOS) SE ote: This applies to access the cools to cools to lava SE, judgment al DOS) SE ote: This applies to access the cools to cools to lava SE, judgment al DOS) SE ote: This applies to access the cools to	ava I I I I I I I I I I I I I I I I I I	https://sty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED-1 041119	
CV Scoring Scal (CVSS)	e 0-1	L	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
			untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail CVSS (CVSS N/UI:	oad and a sted cod omes from net) and a andbox a andbox a vulnerab ploited b specifie onent, ea ervice water ies data a 3.0 Base lability in Vector: S:3.0/AV:	e (e.g., com the rely on the for seculity can be using defined by using thich to the A Score 3 mpacts)	the rity. also APIs ugh a PIs7 . I/PR: A:L).				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Serial versice are Ja 11.0.4 Embe Diffice vulne unaut with multip comp SE En attack vulne unaut cause service Java S Embe	rability in va SE Emple of Oraponent: ization). In that a va SE: 70 ded: 80 de	in the Janbedded acle Java Supportare affectu231, 8th 1221. Coloit allows access woods to ava SE, Java	va la SE ted cted 1221, cker via ava sful lt in of of	https://sty.netapging.com/p-201910001/	p.com ry/nta	O-RED- 041119	
CV Scoring Sca	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	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
			typical sandle applied	deploymally in clapsocations of applets (applets (applets (applets) and asted coordinated by a specific apploited by a specific applets (applets) and a specific applets data	ients run va Web ir sandb in Java S run de (e.g., c om the rely on for secu bility can by using ed e.g., thro which to the A e Score 3 mpacts) T:N/AC:H C:N/I:N/	Start oxed oxed EE 8), code the rity. also APIs ugh a PIs. 7 I/PR: A:L).				
N/A	16-10-2019	4.3	SE prosection SE (construction SE (const	erability oduct of omponer orted ve fected a fand 13 it vulner is unauth is via mu icols to c SE. Succe is vulner it in unau y to caus il of serv of Java S erability deploym	Oracle Jont: 2D). rsions the re Java S. Difficular ability nenticate compronessful attacked ability cathorized a partice (partice). Note: applies to applies applies to applies to applies to applies to applies to applies	ava nat SE: It to ed k nise cacks an d ial cial	https://ty.netap/adviso.p-20193	p.com ry/nta	O-RED- 041119	
CV Scoring Sca	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	D	escription	n & CVE I	D	Pat	ch	NCIIP	CID
			sandbapplication application a	ally in clipoxed Jave cations of applets (in oad and oas sted code and oand oandbox in oad andbox in	va Web sor sandbox san	Start oxed oxed oxed oxed oxed oxed oxed oxed				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with in multicomp SE En attack vulne unaut cause	erability a see En act of Ora ponent: 2 orted verificated and 1, 8u221 va SE En ability at thenticate ple protogrability of thorized a partiace (partial)	in the Janbedded acle Java S2D). rsions the Java S2D, 11.0.4 anbedded access where access where access where S2D, Success ability the denial	ava Il a SE nat SE: and d: cloit cker via Java sful ult in co of	https:// ty.netap /adviso p-2019 0001/	p.com ry/nta	O-RED- 041119	
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
			Embervulne Java of typical sandhat le untru that of interroll Java of This wapply typical load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	E, Java S dded. No rability a leploymo ally in cli boxed Java cations o applets (i boad and sted cod omes fro net) and andbox vulnerab to Java o ally in se and run o (e.g., cod adminis ase Score lability in Vector: S:3.0/AV N/S:U/O D: CVE-	ote: This applies to ents, lents run le (e.g., com the rely on to for seculility does deploymented trustalle trator). Le 3.7 mpacts) :N/AC:H	nning Start oxed E 8), code the rity. es not nents, at sted ed CVSS				
N/A	16-10-2019	4.3	Graal Edition Graal Java). version 19.2.0 vulne unaut with multicomp Graal Edition vulne	erability VM Ente on produ VM (com The sup on that is chenticat network ple proto romise (VM Ente on. While rability is	rprise act of Ora apponents apported affected by to exp allows access v acc	acle d is loit ker via	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
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 P	ublish Date	CVSS	D	escription	ı & CVE II)	Pato	:h	NCIIP	C ID
			significadditics additics success unautic deleticaccess Oracle Editic CVSS (Integration (CVSS N/UI:	on, attackicantly in ional pro- essful attack rability of thorized ion or mo is to critic e GraalV on access 3.0 Base grity imp or: 5:3.0/AV EN/S:C/C	mpact oducts. acks of the can result of the can result of the call data of	lt in n, on or all prise a8 VSS I/PR: A:N).				
N/A 16	5-10-2019	4.3	SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with i multi comp SE En attack vulne unaut cause service Java S Embe	erability and SE Enduct of Orace of Orace of Contents of SE Enduct	nbedded acle Java 2D). rsions the re Java S., 11.0.4 and attact access vectors to ava SE, Java SE, Jav	a SE nat EE: and d: cloit eker via fava sful lt in o of of	https://s ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED-I 041119	
				leploymo	ents,					

Weakness	Publish Dat	e CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			applied Java at that let untrue that continued in term Java so apply typical load at code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	cations of applets (poad and asted coordinate) and andbox vulnerable to Java ally in sea administrate Score lability in Vector: S:3.0/AV	or sandb in Java S run de (e.g., com the rely on for secu- bility doe deploym ervers, the only trust le install strator). e 3.7 mpacts)	oxed EE 8), code the rity. es not nents, nat sted led CVSS				
N/A	16-10-201	4	SE pr SE (co Suppo are af 7u23 13. Dr vulne unaut with r multi comp Succe huma perso attack vulne attack impac produ	erability oduct of omponer orted ve fected a 1, 8u221 ifficult to rability thentical network ple prote romise J essful att in intera on other ker and verability ks may s ct additi- ucts. Suc	Oracle Jont: Javadersions the Java St., 11.0.4 or exploit allows ted attactances woods to cacks received than the while the is in Java ignificancessful	ava loc). nat SE: and cker via quire om a	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	0-RED- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			unautinsert some data a unaut to a staces: vulne Java data that le untru that cointerr Java s This vapply typical load a code (by an 3.0 Ba (Confintegral Vector (CVSS N/UI:	rability of thorized of Java Sas well as thorized ubset of sible dat rability a leployme ally in clip oad and sted cod omes from the Java of the Java	update, te access te access read access read access and access and te ents, tents run le (e.g., com the rely on the rely on the for securility does deploymented the ents all etrator). Le 4.7 ty and acts). CV: N/AC:H: L/I:L/A	to sible cess This counting Start oxed E 8), code che city. ces not ents, at sted ed CVSS SS (/PR: a:N).				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppo are af 7u23: 13; Ja	erability va SE Emuct of Oraponent: 2 ported verificated and 1, 8u221 va SE Emuck.	nbedded acle Java 2D). rsions th re Java S , 11.0.4 nbedded	SE nat E: and	https://sty.netapy/advisorp-20191	p.com y/nta	O-RED- 041119	
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	D	escription	a & CVE II	D	Pate	:h	NCIIF	PC ID
weakness	Publish Date	CVSS	vulne unaut with in multiple composed service Java S Embervulne S Embervu	rability and the theorem is a partial and in the cations of this rability and all points of the cations of the	allows acted attact access to access to ava SE, J . Succes can resu ability t l denial al DOS) acte: This applies t ents run a Web S ar sandb an Java S run acte (e.g., co om the rely on te for secu ility can by using d .g., through to the A Score 3 mpacts) :N/AC:H :N/I:N/	cker via Java sful alt in so of of sto nning Start oxed EE 8), code the rity. also APIs ugh a PIs. J.7 . J./PR: A:L).			NCIII	-CID
N/A	16-10-2019	4.3	SE, Ja produ (com	rability va SE Em ict of Ora conent: irrency)	nbedded acle Java	l a SE	https:// ty.netap /advisor p-20191	p.com cy/nta	O-RED- 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			are Ja 11.0.4 Embe Diffict vulne unaut with r multip comp SE En attack vulne unaut cause servic Java S Embe vulne explor data t specif witho Java V applic Java a throu CVSS (Avail CVSS (CVSS N/UI:	ons that a va SE: 70 and 13; dded: 80 ult to expression of this rability of the control of the c	in 231, 80 is Java SE is Java SE, Java SE, Java SE, Java SE, Java SE, Java SE is Java SE	eker via lava sful lt in o of of s be g ted e7 . I/PR: A:L).	0001/			
N/A	16-10-2019	4.3	SE, Jav produ (comp Suppo are af 7u232	erability in a SE Emuct of Oraponent: Jorted verage of the sected and the sected	nbedded acle Java (AXP). rsions thre Java S , 11.0.4	l a SE nat EE: and	https://s ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
Weakness	Publish Date	CVSS	8u22 vulne unaut with in multi comp SE En attack vulne unaut cause servic Java S Embe vulne Java d typica sandk applic Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avai CVSS (CVSS	escription 1. Difficult rability a chenticate network ple prote romise J nbedded as of this rability a chorized a partia ac (partia	alt to expallows ted attack access to cools to ava SE, Jones ability to denial al DOS) of the content of the co	oloit cker via lava sful lit in of of sto nning Start oxed E 8), code the rity. also APIs ugh a PIs. 7.7	Patc	ch .	NCIIP	PC ID
			Í	D : CVE -						
N/A	16-10-2019	5.8	SE, Ja produ	rability va SE En ict of Ora ponent: S	nbedded acle Java	l a SE	https://s ty.netap /advisor p-20191	p.com y/nta	0-RED- 041119	
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
			Supported versions that	0001/	
			are affected are Java SE:		
			8u221, 11.0.4 and 13; Java		
			SE Embedded: 8u221.		
			Difficult to exploit		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			multiple protocols to		
			compromise Java SE, Java		
			SE Embedded. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Java SE, Java SE		
			Embedded accessible data		
			and unauthorized ability		
			to cause a partial denial of		
			service (partial DOS) of		
			Java SE, Java SE		
			Embedded. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			,		
			This vulnerability can also		
			be exploited by using APIs		
			in the specified		
			Component, e.g., through a		
			web service which		
			supplies data to the APIs.		
			CVSS 3.0 Base Score 4.8		
			(Integrity and Availability		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L). CVE ID : CVE-2019-2975		
enterprise_l	inux_server				
N/A	16-10-2019	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	O-RED-ENTE- 041119/1116

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			This vapply typical load a code by an 3.0 Ba (Avail CVSS (CVSS N/UI:	andbox to Java of ally in second administrations are Score ability in Vector: 1:3.0/AV R/S:U/C D: CVE-	ility doe deploym rvers, the only trus e install trator). e 3.1 mpacts) :N/AC:H	es not tents, tat sted ed CVSS				
N/A	16-10-2019	4.3	SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with a Kerber Sember vulne Java Sember vulne unaut critica access SE En data. vulne	rability is a SE Emporent: I ported verifected and I, 8u221 and SE Emporent is a SE Emporent in the section of	nbedded acle Java Kerbero rsions the re Java S , 11.0.4 abedded attacked at	s SE s). at E: and d: bloit ker ria aise tacks act his lt in o ete ava ole	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED-1 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	CID
			sandbapplications application	ally in clipoxed Jave cations of applets (in pad and sted code omes from the categories of an andbox evaluerable ploited be specified by a specified onent, end and box evaluerable onent, end as data 3.0 Base didentiality Vector: S:3.0/AV N/S:C/C	va Web sor sandbox san	Start oxed oxed oxed oxed oxed oxed oxed oxed				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with multicomp SE En attack vulne unaut cause	rability a SE Em act of Ora ponent: I ported verificated and 1, 8u221 va SE Em 1. Difficut rability a chenticate protes of this rability of chorized a partial ce (partial ce	in the Janbedded acle Java Serial 1.0.4 abedded access where allows access where access	va I I SE king). nat SE: and d: cloit ker via Java sful co of	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	PC ID
			Embervulne Java of typical sandhapplical Java and that lead that l	E, Java S dded. No rability a leployme ally in cli boxed Jav cations o applets (i boad and asted cod omes fro net) and candbox vulnerab ploited b e specifie bonent, e service w ies data 3.0 Base lability in Vector: 5:3.0/AV N/S:U/O D: CVE-	ote: This applies to ents, lents run le (e.g., com the rely on the rely on the lility can by using degree 3 mpacts) :N/AC:H	nning Start oxed E 8), code the rity. also APIs ugh a PIs. 5.7				
N/A	16-10-2019	4.3	SE, Japrodu (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En	erability va SE En let of Ora ponent: J orted ver fected an 1, 8u221 va SE En thenticat network ple proto romise J nbedded	nbedded acle Java (AXP). rsions the re Java S ., 11.0.4 nbedded alt to exp allows access to access to ava SE, J . Succes	l a SE nat SE: and d: oloit cker via	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			unaut cause service Java S Embe vulne Java d typica sandh applie Java a that le untru that c interregion Java s This very be expired the Competer Supple CVSS (Avail CVSS (CVSS N/UI:	rability of thorized a partial ce (partial ce). Java Sedded. No rability a leployment of the control of the con	ability to l denial al DOS) of SE ote: This applies to ents, dents run le (e.g., com the rely on the rely on the lility can by using downlich to the A secore 3 mpacts) :N/AC:H	of of of of sto oning Start oxed SE 8), code the rity. also APIs ugh a PIs. 5.7 .				
N/A	16-10-2019	4.3	SE, Jar produ (comp Serial version are Ja 11.0.4 Embe Diffict vulne	erability ava SE Emact of Oraponent: lization). ons that ava SE: 70 and 13 edded: 80 ult to exprability at the enticat	nbedded acle Java . Suppor are affec u231, 8u ; Java SE u221. ploit allows	ted cted 1221,	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
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	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			multip compose SE Emattack vulne unaut cause service Java S Embe vulne Java d typica sandb applice Java a that le untru that content Java s This vole expin the Compose Supplice CVSS (Avail CVSS (CVSS N/UI:	network ple proto romise Ja bedded as of this rability of a partial a partia	can resurability to denial al DOS) of the contract of the cont	Java sful alt in so of of sto ming Start oxed SE 8), sode the rity. also APIs ugh a PIs. 5.7 .				
N/A	16-10-2019	4.3	SE pro SE (co Suppo are af 11.0.4	erability in oduct of omponer orted verificated and 13. it vulner	Oracle J nt: 2D). rsions th re Java S . Difficul	ava nat E:	https://sty.netapy/advisorp-201910001/	p.com ry/nta	O-RED- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			attackaccess proto Java S of this result ability denia DOS) vulne Java de typica sandkapplic Java athat le untru that content Java s This was This was the explication of the Compweb s supplice CVSS (Avail CVSS (CVSS N/UI:	s unauth ser with so via mulcols to constant of service with and sted code omes from the control and box rulnerable ploited be specified and sted code and sted code omes from the control and box rulnerable ploited be specified and sted code and sted code and sted code omes from the control and box rulnerable ploited be specified and sted code and ste	networl ltiple ompron essful att ability ca thorized a part ice (part EE. Note: applies t ents, ients run le (e.g., c om the rely on t for secu ality can by using ed eg, throu which to the A e Score 3 mpacts) EN/AC:H E:N/I:N/	nise cacks an d ial cial This co nning Start oxed E 8), code the rity. also APIs ugh a PIs7 . I/PR: A:L).				
N/A	16-10-2019	4.3	SE, Japrodu (comp Suppo are af 7u23	erability va SE En oct of Ora ponent: 2 orted ver fected ar 1, 8u221 va SE En	nbedded acle Java 2D). rsions thre Java S	l a SE nat SE: and	https://sty.netapy/advisorp-20191	p.com y/nta	O-RED- 041119	
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	D	escription	a & CVE I	D	Pato	:h	NCIIP	CID
			8u22	1. Difficu	lt to exp	oloit				
			vulne	rability a	allows					
			unaut	henticat	ed attac	cker				
			with 1	network	access v	<i>r</i> ia				
			multi	ple proto	cols to					
			comp	romise J	ava SE,]	Java				
			SE En	nbedded	. Succes	sful				
			attacl	s of this						
			vulne	rability (can resu	lt in				
			unaut	horized	ability t	.0				
			cause	a partia	l denial	of				
			servi	e (partia	al DOS)	of				
			Java S	E, Java S	E					
			Embe	dded. No	ote: This	S				
				rability a		to				
				leploym	•					
				ılly in cli		_				
				oxed Jav						
			appli	cations o	r sandb	oxed				
			-	pplets (i	-	SE 8),				
				oad and						
				sted cod		code				
				omes fro						
				net) and	-					
				andbox		-				
				ulnerab -	,					
				to Java						
				ally in se						
				ind run o	•					
				(e.g., cod						
			-	adminis	-	CVSS				
				ase Score						
			-	lability ii	mpacts)					
				Vector:	NI / 4 G T	I /DD				
			-	5:3.0/AV	-	-				
			N/UI:	N/S:U/C	:N/I:N/	A:L).				
			CVE I	D : CVE-	2019-2	988				
			Vulne	rability	in the Oracle https://secur			securi		
N/A	16-10-2019	4.3	Graal	VM Ente	rprise		ty.netap	p.com	O-RED-	
,				n produ			/advisor		041119	/1123
			Graal	VM (com	ponent	<u>: </u>	p-20191	.017-		
CV Scoring Sca	ole 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				5-4	- 7 3	30		, 0	0 9	J 10

Weakness	Publish Date	cvss	D	escription	ո & CVE II	D	Pato	h	NCIIP	CID
			Java). versice 19.2.0 vulne unaut with in multi comp Graal Editice vulne Graal Editice signif additi Succe vulne unaut deleti access Oracle Editice CVSS (Integ Vecto (CVSS N/UI:	The sup on that is 2. Difficult a chenticate the protocomise (Constitution) of the protocomise (Constitution	ported saffected to expallows sed attace access we cools to Dracle rprise sis in Orar prise at the can resurrent oducts. acks of the can resurrent odification odification of the can sible data of the can resurrent of th	d is cloit eker via cle chis lt in on or all prise a. v.8 v.S.	0001/			
N/A	16-10-2019	4.3	SE, Japrodu (composupped are af 7u23: 13; Ja 8u22: vulne unaut with i	rability wa SE Emact of Oracted verificated and SE Emack. Difficular ability and setwork ple protogen	nbedded acle Java 2D). rsions the re Java S , 11.0.4 nbedded alt to exp allows red attact access v	l a SE aat EE: and d: oloit	https://s ty.netapy /advisor p-20191 0001/	p.com ry/nta	O-RED- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			SE En attack vulne unaut cause service Java S Embe vulne Java d typica sandh applie Java a that le untru that c interregion Java s This vapply typica load a code (by an 3.0 Ba (Avail CVSS (CVSS N/UI:	romise Jabedded as of this rability of thorized a partial as (partial as (part	can resurability to ability to ability to all DOS) of Epote: This applies to ents, ents runder (e.g., compared to a le (e.g.,	sful It in o of of of start oxed E 8), code the rity. code the rest not nents, nat sted ed CVSS				
N/A	16-10-2019	4	SE pro SE (co Suppo are af 7u233 13. Di vulne	erability in the control of the cont	Oracle J nt: Javad rsions th re Java S , 11.0.4 o exploit allows	ava oc). aat E: and	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED- 041119	
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
			with network access via		
			multiple protocols to		
			compromise Java SE.		
			Successful attacks require		
			human interaction from a		
			person other than the		
			attacker and while the		
			vulnerability is in Java SE,		
			attacks may significantly		
			impact additional		
			products. Successful		
			attacks of this		
			vulnerability can result in		
			unauthorized update,		
			insert or delete access to		
			some of Java SE accessible		
			data as well as		
			unauthorized read access		
			to a subset of Java SE		
			accessible data. Note: This		
			vulnerability applies to		
			Java deployments,		
			typically in clients running		
			sandboxed Java Web Start		
			applications or sandboxed		
			Java applets (in Java SE 8),		
			that load and run		
			untrusted code (e.g., code		
			that comes from the		
			internet) and rely on the		
			Java sandbox for security.		
			This vulnerability does not		
			apply to Java deployments,		
			typically in servers, that		
			load and run only trusted		
			code (e.g., code installed		
			by an administrator). CVSS		
			3.0 Base Score 4.7		
			(Confidentiality and		
			Integrity impacts). CVSS		
			Vector:		
			v CCtO1.		

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			N/UI:	5:3.0/AV R/S:C/C D : CVE-	:L/I:L/ <i>A</i>	λ:N).				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppor are af 7u23 13; Ja 8u22 vulne unaut with a multi comp SE En attack vulne unaut cause service Java SEmber vulne Java of typica sandk application application of the total formattic formattic service service service Java SEmber vulne Java of typica sandk application application of the total formattic service s	erability va SE En oct of Ora ponent: 2 ponenticat network ple proto rability oct horized a partia ce (partia ce (partia ce (partia ce (partia ce) ponenticat poxed Jav cations oc pplets (i poxed Jav c	acle Java 2D). rsions the Java S, 11.0.4 abdeded attack access to ava SE, J. Success ability to ability to a Java S and bear and	a SE at SE: and d: cloit cker via at sful dit in co of sto nning Start oxed EE 8), code the rity. also APIs	https://sty.netapy/advisorp-201910001/	p.com ry/nta	O-RED-1 041119	
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	D	escription	& CVE II)	Pato	h	NCIIP	CID
			CVSS (Avail CVSS (CVSS N/UI:	ies data 3.0 Base lability in Vector: 5:3.0/AV N/S:U/C D: CVE- rability:	Score 3 mpacts). :N/AC:H ::N/I:N/. 2019-2	.7 /PR: A:L). 962				
N/A	16-10-2019	4.3	SE, Jar produ (comp Concurversion are Ja 11.0.4 Ember Diffict vulne unaut with a multiple comp SE En attack vulne unaut cause service Java SE Ember vulne explodata to specific without Java Vapplice Java a througe CVSS	va SE Enact of Oraconent: arrency) ons that a va SE: 70 and 13 dded: 80 alt to exprability a chenticate protocomise Jabedded as of this rability of the chorized a partial ace (partial E, Java S dded. No rability of the Star cations of pplets, sigh a web 3.0 Base	Supporare affect 1231, 8ud 1331, 8ud	ker ria ava sful lt in o of be g	https://ty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED-1 041119	
				<u> </u>	<u> </u>					

Weakness	Publish Date	CVSS	D	escriptior	& CVE II	D	Pato	h	NCIIP	C ID
			(CVSS N/UI:	Vector: 5:3.0/AV N/S:U/C D : CVE-	:N/I:N/	A:L).				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppor are af 7u23: 13; Ja 8u22: vulne unaut with a multip comp SE En attack vulne unaut cause service Java S Embe vulne Java d typica sandb applie Java a that le untru that c interrulava s This very in the	erability in a SE Emponent: Jorted verificated and a partial and a partial are (partial a partial a partia	in the Janbedded AXP). The Java Strain resurcability to the Idential al DOS) of Expelies to the Tay and Strain Java Strain resurca Web Strain Java Str	va I SE I at E: and I: bloit Eker via I so	https://sty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED-1 041119	
CV Scoring Sca										

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			suppl CVSS (Avai CVSS (CVSS N/UI: CVE I	ies data 3.0 Base lability in Vector: 5:3.0/AV N/S:U/C D: CVE-	to the A Score 3 mpacts) :N/AC:H ::N/I:N/ 2019-2 in the Ja	.7 I/PR: A:L). 973 va				
N/A	16-10-2019	5.8	produ (com) Suppo are af 8u22 SE En Diffic vulne unaut with a multi comp SE En attack vulne unaut insert some Embe and u to cau service Java S Embe vulne java S Enda applica java a	va SE En act of Oraponent: Sorted verificated and and and are specially in clipoxed Java Sedded. No actions of Java Sedded according in clipoxed Java Sedded. No actions of Java Sedded and actions of Java Sedded. No actions of Java Sedded. No actions of Java Sedded and actions of Java Sedded. No actions of Java Sedded.	acle Java Scripting rsions the re Java S and 13; : 8u221 ploit allows red attace access v pocols to ava SE, J . Succes can resu update, re access EE, Java S cessible ized abilitial deni al DOS) EE pte: This applies tents, ents run va Web S r sandb in Java S	s SE g). nat sE: Java sker via sful lt in s to SE data lity ial of of so nning Start oxed	https://ty.netap/advisorp-20191	p.com ry/nta	O-RED- 041119	
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	De	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			that co intern Java sa This v be exp in the Comp web sa suppli CVSS : (Integ impac (CVSS N/UI:	omes fromes fromes from and box rulneraboloited by specifie onent, everyice was data 3.0 Base rity and tts). CVS:3.0/AVN/S:U/O	rely on for secu ility can by using d .g., thro	the rity. a also APIs ugh a .PIs. 4.8 bility r: H/PR: A:L).				
enterprise li	nux_workstati	ion	CVE	D: CVE-	2019-2	9/3				
N/A	16-10-2019	2.6	SE, Jav produ (comp Suppo are aff 7u231 13; Jav 8u221 vulner unaut with r multip compr SE Em attack intera other Succes vulner unaut cause	va SE Enact of Oract	ted attac access v	d SE king). nat SE: and d: ploit cker via Java esful n rson er. this ult in to of	https://s ty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED-1 041119	
CV Scoring Sca	le 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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
			Embervulne Java of typical sandhat le untru that of interred Java sandhat le untru that of inter	EE, Java Sedded. No rability a leploymonally in clipoxed Java Cations of applets (in and box and box and box and run of administic Section (e.g., code admi	ote: This applies to ents, lents run le (e.g., com the rely on to litty does deploymented trustalle trator). Le 3.1 mpacts) :N/AC:H. C:N/I:N/AC:H.	anning Start oxed E 8), code the rity. es not nents, at sted ed CVSS				
N/A	16-10-2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with the Kerbe Java S Embe	erability va SE En oct of Ora ponent: l orted ver fected an 1, 8u221 va SE En 1. Difficu rability a chenticat network eros to co sE, Java S edded. W rability i	nbedded acle Java Kerbero rsions the Java Son 11.0.4 allows access when the first to expend access when the first to expend access when the first	s). s). nat E: and d: cloit eker via	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			may sadditic Succes vulne unaut critical access. SE Endata. vulne Java data interrulate interrulate sanditical applical sanditical applical sanditical formulate continuity in the explication of the Composition of the Compo	E Embedignificar ional properties and attack the code and attack the code and attack the code and and box explets (in the code and box explositely (in the code and box explositely (in the code and box explositely (in the code and box ex	ntly impoducts. acks of to can result access to comple accessibilities applies to ents run le (e.g., com the rely on the rely on the rely on the for secultity can by using a downless to the Accessibility can be a secultive to the Accessibility can be a secured to the Accessibility can be a secured to	chis It in o ete ava ble co nning Start oxed E 8), code the rity. also APIs ugh a PIs. 8 cts).				
N/A	16-10-2019	4.3	SE, Japrodu (comp Suppo are af 7u23	erability or SE En oct of Ora ponent: I ported ver fected an 1, 8u221 va SE En	nbedded acle Java Network rsions thre Java S ., 11.0.4	l s SE king). nat SE: and	https:// ty.netap /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
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	D	escription	n & CVE I	D	Pato	h	NCIIP	CID
Weakness	Publish Date	CVSS	8u22 vulne unaut with in multi comp SE En attack vulne unaut cause servic Java S Embe vulne Java o typica sandk applic Java a that le untru that c interr Java s This v be exp in the Comp web s suppl CVSS (Avail	1. Difficult rability a chenticate protocomise Judged ded control and cations of a partial ca	alt to expallows aced attack access to cools to ava SE, J. Success ability to the all DOS) and the common the rely on the rely	ploit cker via Java sful alt in co of sto nning Start oxed EE 8), code the rity. also APIs ugh a PIs. 3.7	Pato	ch	NCIIP	CID
			(CVSS N/UI:	S:3.0/AV N/S:U/C D : CVE-	:N/I:N/	A:L).				
N/A	16-10-2019	4.3	Vulne SE, Ja produ	erability va SE En uct of Ora ponent:]	in the Ja nbedded acle Java	iva l	https:// ty.netap /advisor p-20191	p.com y/nta	O-RED- 041119	
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/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	O-RED-ENTE- 041119/1134

Weakness	Publish Date	CVSS	D	escription	& CVE II	D	Pato	:h	NCIIP	C ID
Weakness	Publish Date	CVSS	(Avail CVSS (CVSS N/UI: CVE I Vulne SE pro SE (co Suppo are af 11.0.4 explo allow attack access proto Java S of this result ability denia	escription lability in Vector: S:3.0/AV: S:3.0/AV: Constant of Perability in Outed very oduct of Omponer orted very fected and and 13. it vulner is unauth is via mult cols to co SE. Succe is vulnera it in unau y to caus l of servi of Java S	mpacts). :N/AC:H ::N/I:N/. 2019-2 in the Ja Oracle Java S : Difficult rability enticate network ltiple ompromissful att ability cat thorized e a particle ice (part	I/PR: A:L). 983 va ava at EE: t to ed k aise cacks an d ial cial	https://s	securi		
N/A	16-10-2019	4.3	Java de typica sandba applied Java a that le untru that ce interred Java so This was be explicated to the Compose web soupple CVSS	rability a deployment ally in clipoxed Javes ations of a pplets (in oad and in oad and in oad and in oad and in oad and box in oad and in	ents, ents run va Web S r sandbe in Java S run le (e.g., c om the rely on t for secur ility can by using le d le g., throughich to the Al Score 3	nning Start oxed EE 8), code the rity. also APIs ugh a PIs.	/advisor p-20191 0001/		0-RED-1 041119	
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 N/UI:	Vector: 5:3.0/AV N/S:U/C D : CVE-	:N/I:N/	A:L).				
N/A 16-10-3	2019	4.3	SE, Ja produ (comp Suppo are af 7u23 13; Ja 8u22 vulne unaut with multi comp SE En attack vulne unaut cause service Java S Embe vulne Java S Embe vulne Java S This varies apply typica	erability in clipated and box of this cations of this cations of the cations of t	nbedded acle Java 2D). rsions the Java S., 11.0.4 inbedded attack access to ava SE, J. Success ability to denial al DOS). SE cote: This applies to ents, lents run le (e.g., com the rely on for secuility does deploymervers, the rest of the secuility does deploymervers, the rest of the secuility does deploymervers, the rely on the	a SE nat SE: and d: cloit cker via Java sful dt in co of sto nning Start oxed SE 8), code the rity. es not nents, nat	https://sty.netapj /advisor p-20191 0001/	p.com ry/nta	O-RED-1 041119	
CV Scoring Scale (CVSS)	-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS.3.0/AV:N/AC:H/PR: N/U:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988 Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). The supported version that is affected is 19.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data. CVSS 3.0 Base Score 6.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/U:N/S:C/C:N/I:H/A:N). CVE ID: CVE-2019-2989	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). The supported version that is affected is 19.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data. CVSS 3.0 Base Score 6.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:C/C:N/I:H/A:N).				by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2988		
	N/A	16-10-2019	4.3	GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). The supported version that is affected is 19.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data. CVSS 3.0 Base Score 6.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:C/C:N/I:H/A:N).	ty.netapp.com /advisory/nta p-20191017-	

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts).	https://securi ty.netapp.com /advisory/nta p-20191017- 0001/	O-RED-ENTE- 041119/1138

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:N/A:L). CVE ID: CVE-2019-2992 Vulnerability in the Java SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13. Difficult to exploit	
SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and	
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional 16-10-2019 4 impact additional O-RED	D-ENTE- 19/1139
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			interr Java s This v apply typica load a code by an 3.0 Ba (Conf Integr Vecto (CVSS N/UI:	omes fromet) and andbox to Java on the Jav	rely on to for secu- ility doe- deploymervers, the only trusted e installed e trator). e 4.7 ty and ects). CV :N/AC:H :L/I:L/A	rity. es not nents, nat ested ed CVSS				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with multicomp SE En attack vulne unaut cause service Java SEmbe vulne Java de J	rability va SE En oct of Ora conent: 2 orted ver fected an 1, 8u221 va SE En 1. Difficu- rability a chenticat network ple proto romise J nbedded as of this rability o chorized a partia ce (partia de, Java S dded, No rability a leploymo	in the Janbedded acle Java 2D). rsions the Java Song in	va la SE nat le: and l: oloit leker via ava sful lt in of of	https://s ty.netapy /advisor p-20191 0001/	p.com y/nta	O-RED- 041119	
CV Scoring Sca										

Weakness	Publish Date	cvss	D	escription	ı & CVE I	D	Pato	h	NCIIP	CID
			applied Java at that let untrue that continued in the Comparent of the Com	cations of applets (in oad and and and and and and and and and a	r sandb in Java S run le (e.g., com the rely on for secu ility can by using d lg., through to the A Score 3 mpacts) :N/AC:H	oxed SE 8), code the rity. also APIs ugh a PIs. 3.7				
N/A	16-10-2019	4.3	Vulnes SE, Ja produ (comp Concu versic are Ja 11.0.4 Embe Diffic vulne unaut with i multi comp SE En attack vulne unaut cause	erability va SE Emuct of Oraponent: arrency) ons that a va SE: 70 and 13 edded: 80 and 13 ethenticate ple protographic of this erability of thorized a partiace (partial	in the Janbedded acle Java Support are affect 1231, 8th 1221. ploit allows access to access to ava SE, Java SE	rted cted u221, cker via Java sful	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED- 041119	
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	D	escription	ı & CVE II	D	Pato	h	NCIIP	CID
			Emberoulne explored data to specific without Java Wapplic Java athrout CVSS (Avail CVSS (CVSS N/UI:	EE, Java Sedded. No rability of ited by second complets, second complete,	ote: This can only upplying the ponent Untrust t r Untrus occurrence Score 3 mpacts). :N/AC:H	ted sted c7 . I/PR: A:L).				
N/A	16-10-2019	4.3	Vulne SE, Jar produ (comp Suppo are af 7u23: 13; Ja 8u22: vulne unaut with multip comp SE En attack vulne unaut cause service Java S Embe vulne	erability in va SE Emuct of Oraponent: Jorted vention of Emula of	in the Janbedded acle Java (AXP). The Java Serial of the Earl of t	va l a SE nat EE: and d: cloit eker via fava sful dt in of of	https://s ty.netapy /advisor p-20191 0001/	p.com ry/nta	0-RED- 041119	
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	D	escription	n & CVE I	D	Pate	ch	NCIIP	CID
			sandbapplicallians applicallians application applicati	ally in clipoxed Jave cations of applets (in oad and asted code and andbox andbox andbox andbox andbox are conent, eare cate at a 3.0 Base lability in Vector: 5:3.0/AV N/S:U/C	va Web Sor sandbox san	Start oxed oxed oxed oxed oxed oxed oxed oxed				
N/A	16-10-2019	5.8	Vulne SE, Jar produ (comp Suppo are af 8u22: SE En Diffict vulne unaut with the multiple comp SE En attack vulne unaut insert	erability a va SE Emuct of Ora ponent: Se or ted verability a chemical metwork ple protogrability a chorized tor delete of Java Se or delete or delet	in the Janbedded acle Java Scripting rsions the re Java Stand 13; and 13; allows access woods to ava SE, Java S	tva It	https:// ty.netap /advisor p-20191 0001/	p.com ry/nta	O-RED- 041119	
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
			Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: N/UI:N/S:U/C:N/I:L/A:L).			
Ricoh						
mp_501_firm	ware					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	On the RICOH MP 501 printer, HTML Injection and Stored XSS vulnerabilities have been discovered in the area of adding addresses via the entryNameIn and KeyDisplay parameter to /web/entry/en/address/a	N/A		O-RIC-MP_5- 041119/1144
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 684	6-7 7	7-8	8-9 9-10

Weakness	Pu	blish Date	CVSS	D	escriptio	n & CVE I	D	Pato	ch	NCIIP	CID
				drsSe	tUserWi	izard.cgi					
					D : CVE-	2019-					
				1820	3						
Samsung											
galaxy_s10_fi	rmv	vare		_							
Improper Input Validation	17-	10-2019	4.4	Samsung Galaxy S10 and Note10 devices allow unlock operations via unregistered fingerprints in certain situations involving a third-party screen protector. CVE ID: CVE-2019-17668		N/A		0-SAM- 041119			
note_10_firm	war	e									
Improper Input Validation	17-	10-2019	4.4	Samsung Galaxy S10 and Note10 devices allow unlock operations via unregistered fingerprints in certain situations involving a third-party screen protector. CVE ID: CVE-2019-17668		N/A		O-SAM- 041119			
Sangoma											
session_bord	er_c	ontrolle	r_firmw	are							
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component ('Injection')		10-2019	5	The Sangoma Session Border Controller (SBC) 2.3.23-119 GA web interface is vulnerable to Argument Injection via special characters in the username field. Upon successful exploitation, a remote unauthenticated user can create a local system user with sudo privileges, and use that		N/A		0-SAN- 041119			
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	D	escription	1 & CVE II	D	P	atch	NCIIP	C ID
			(either via the web interface or via SSH) to achieve complete compromise of the device. This affects /var/webconfig/gui/Webc onfig.inc.php and /usr/local/sng/bin/sng-user-mgmt. CVE ID: CVE-2019-12147 The Sangoma Session							
Improper Authenticati on	22-10-2019	7.5	The Sangoma Session Border Controller (SBC) 2.3.23-119 GA web interface is vulnerable to an authentication bypass via an argument injection vulnerability involving special characters in the username field. Upon		N/A		0-SAN- 041119			
terra-master			12148							
f2-210_firmw										
Improper Privilege Managemen t	28-10-2019	6.5	An issue was discovered on TerraMaster FS-210 4.0.19 devices. Normal users can use 1.user.php for privilege elevation. CVE ID: CVE-2019-			.0 il ohp	N/A		O-TER- 041119	
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	Puk	olish Date	cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
				1819	5						
fs-210_firmw	are										
Information Exposure Through Log Files	23-2	10-2019	5	An issue was discovered on TerraMaster FS-210 4.0.19 devices. An unauthenticated attacker can download log files via the include/makecvs.php?Eve nt= substring. CVE ID: CVE-2019-18385				N/A		O-TER- 041119	
Tp-link											
m7350_firmy	ware										
Improper											
Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-2	10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow externalPort OS Command Injection (issue 1 of 5). CVE ID: CVE-2019-13649				N/A		O-TPM735- 041119/1151	
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-2	10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow internalPort OS Command Injection (issue 2 of 5). CVE ID: CVE-2019-13650			N/A		O-TPN 041119		
Improper Neutralizati on of Special Elements used in an	24-1	10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow portMappingProtocol OS Command Injection (issue			N/A		O-TPM735- 041119/1153		
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	ı	NCIIP	C ID
OS Command ('OS Command Injection')			3 of 5). CVE ID: CVE-2019- 13651				
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow serviceName OS Command Injection (issue 4 of 5). CVE ID: CVE-2019-13652	N/A		O-TPM 041119	
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow triggerPort OS Command Injection (issue 5 of 5). CVE ID: CVE-2019-13653	N/A		O-TPM 041119	
Wago							
pfc200_firmv	vare						
Externally Controlled Reference to a Resource in Another Sphere	19-10-2019	5	Information Disclosure is possible on WAGO Series PFC100 and PFC200 devices before FW12 due to improper access control. A remote attacker can check for the existence of paths and file names via crafted HTTP requests. CVE ID: CVE-2019-18202	N/A		0-WAG- 041119	
pfc100_firmv	ware						
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 688	6-7	7-8	8-9	9-10

Externally Controlled	Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
Tardware	Controlled Reference to a Resource in Another	19-10-2019	5	possi PFC1 devic to im contr can cl of pat	ble on W 00 and P es before proper a ol. A ren neck for ths and f	YAGO Se PFC200 e FW12 access note atta the exis	due acker tence	N/A			
Tog_zephyrus_m_gm501gs *** DISPUTED ** The BIOS configuration design on ASUS ROG Zephyrus M GM501GS laptops with BIOS 313 relies on the main battery instead of using a CMOS battery, which reduces the value of a protection mechanism in which booting from a USB device is prohibited. Attackers who have physical laptop access can exhaust the main battery to reset the BIOS configuration, and then achieve direct access to the hard drive by booting a live USB OS without disassembling the laptop. NOTE: the vendor has apparently indicated that this is "normal" and use of						2019-					
** DISPUTED ** The BIOS configuration design on ASUS ROG Zephyrus M GM501GS laptops with BIOS 313 relies on the main battery instead of using a CMOS battery, which reduces the value of a protection mechanism in which booting from a USB device is prohibited. Attackers who have physical laptop access can exhaust the main battery to reset the BIOS configuration, and then achieve direct access to the hard drive by booting a live USB OS without disassembling the laptop. NOTE: the vendor has apparently indicated that this is "normal" and use of				1020		are					
** DISPUTED ** The BIOS configuration design on ASUS ROG Zephyrus M GM501GS laptops with BIOS 313 relies on the main battery instead of using a CMOS battery, which reduces the value of a protection mechanism in which booting from a USB device is prohibited. Attackers who have physical laptop access can exhaust the main battery to reset the BIOS configuration, and then achieve direct access to the hard drive by booting a live USB OS without disassembling the laptop. NOTE: the vendor has apparently indicated that this is "normal" and use of											
Improper Input Validation 20-10-2019 7.2 Configuration design on ASUS ROG Zephyrus M GM501GS laptops with BIOS 313 relies on the main battery instead of using a CMOS battery, which reduces the value of a protection mechanism in which booting from a USB device is prohibited. Attackers who have physical laptop access can exhaust the main battery to reset the BIOS configuration, and then achieve direct access to the hard drive by booting a live USB OS without disassembling the laptop. NOTE: the vendor has apparently indicated that this is "normal" and use of	rog_zephyrus	s_m_gm501gs									
the same battery for the BIOS and the overall system is a "new design."	Input	20-10-2019	7.2	config ASUS GM50 BIOS main using which a pro- which devic Attach physi exhau to res config achie the ha a live disass NOTE appar this is the sa BIOS	guration ROG Zep 11GS lap 313 relic battery a CMOS a reduce tection in booting e is prob kers who cal lapto ast the in guration we direct ard drive ard drive uSB OS sembling tently in s "norma ame batt and the	design of phyrus Natops with es on the instead of battery is the value of have on a ccess and the taccess of by boo without ing the lapendor has dicated of and under year and under year and under year and under and u	on M ch e of , lue of sm in USB s can tery en to ting to ting that lse of che	N/A			
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	_	le 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			However, the vendor apparently plans to "improve" this an unspecified later time. CVE ID: CVE-2019-18216		
avstar					
pe204					
Improper Input Validation	23-10-2019	5	An issue was discovered on AVStar PE204 3.10.70 IP camera devices. A denial of service can occur on open TCP port 23456. After a TELNET connection, no TCP ports are open. CVE ID: CVE-2019-18382	N/A	H-AVS-PE20- 041119/1159
Bitdefender					
box					
Allocation of Resources Without Limits or Throttling	17-10-2019	4.9	An issue was discovered in Bitdefender BOX firmware versions before 2.1.37.37-34 that affects the general reliability of the product. Specially crafted packets sent to the miniupnpd implementation in result in the device allocating memory without freeing it later. This behavior can cause the miniupnpd component to crash or to trigger a device reboot. CVE ID: CVE-2019-12611	N/A	H-BIT-BOX- 041119/1160
Cisco	<u> </u>			l	

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	1-2	7	†) †	3-0	0-7	7	5	J-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
webex_board	1_55				
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an affected device. CVE ID: CVE-2019-15962	N/A	H-CIS-WEBE- 041119/1161
webex_board	l_55s				
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an affected device. CVE ID: CVE-2019-	N/A	H-CIS-WEBE- 041119/1162

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			1596	2						
webex_board	1_70									
Incorrect Default Permissions	16-10-2019	6.6	of Cis Colla (CE) an au attack the /s affect vulne assign could vulne as the and v /root affect	assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an affected device. CVE ID: CVE-2019-15962 A vulnerability in the CLI		N/A		H-CIS-W 041119		
webex_board	l_70s									
Incorrect Default Permissions	16-10-2019	6.6	of Cis Colla (CE) an au attach the /i affect vulne assign could vulne as the and v	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an			N/A		H-CIS-W 041119	
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019- 15962		
webex_board	d_85s				
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an affected device. CVE ID: CVE-2019-15962	N/A	H-CIS-WEBE- 041119/1165
webex_room	_55				
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an	N/A	H-CIS-WEBE- 041119/1166

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & C\	/E ID	Pato	h	NCIIP	C ID
			affected device. CVE ID : CVE-2019 15962	9-				
webex_room_	_55_dual							
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in to of Cisco TelePreser Collaboration Endposition (CE) Software could an authenticated, lattacker to write fit the /root directory affected device. The vulnerability is during the exploit this vulnerability by logasthe remotesupper and writing files to /root directory of affected device. CVE ID: CVE-2019	nce point d allow ocal les to v of an e e to on acker gging in ort user o the an	N/A		H-CIS-W 041119	
			15962					
webex_room_	_70_dual							
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in to of Cisco TelePreser Collaboration Endposed (CE) Software could an authenticated, lattacker to write fitthe /root directory affected device. The vulnerability is due improper permissing assignment. An attacker to write fitthe /root directory affected device. The vulnerability is due improper permissing assignment. An attacker to write in the vulnerability by logas the remotesupp and writing files to	nce point d allow ocal les to v of an e e to on acker gging in ort user	N/A		H-CIS-W 041119	
CV Scoring Scal	le <u>0-1</u>	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			affect	director ed devic	ce.					
			1596	D : CVE- 2	-2019-					
webex_room	_70_dual_g2									
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user and writing files to the /root directory of an affected device. CVE ID: CVE-2019-15962				N/A		H-CIS-W 041119	
webex_room	_70_single									
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in as the remotesupport user			nt nlllow al to an	N/A		H-CIS-W 041119	
CV Scoring Sca	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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			/root affect CVE I	vriting find director and device the control and the control by the control cont	ry of an ce.	e				
wahay room	_70_single_g2		1596	2						
Incorrect Default Permissions	16-10-2019	6.6	of Cis Collal (CE) S an au attack the /n affect vulne impro assign could vulne as the and w /root	nerability contention of the nerability oper per nament. A exploit erability eremote viting fired deviced devi	Presence Endpoid could a ted, located, located files ectory of te. The tis due to mission an attack this by loggin support les to th ry of an	nt Illow Il to an eer	N/A		H-CIS-W 041119	
			1596	D : CVE	-2019-					
webex_room	_kit									
Incorrect Default Permissions	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to write files to the /root directory of an affected device. The vulnerability is due to improper permission assignment. An attacker could exploit this vulnerability by logging in			nt Illow Il to an	N/A		H-CIS-V 041119	
CV Scoring Sca	le <u>0-1</u>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pul	blish Date	cvss	D	escriptio	n & CVE I	D		Pato	h	NCIIP	CID
				and w /root affect	e remote vriting fi director ed device D : CVE- 2	les to th ry of an ee.						
firepower_m	anag	gement_	center_1	.000								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execute code interf sensitinform	ple vuln eb-base gement Firepow gement) could a enticated car to co site scri cagainst based m face. The rabilitie ficient va supplied based m face. An a exploit rabilitie ading a face to cl A success allow th te arbita in the co face or a ctive, bro mation. D: CVE- 8	interfactiver Center Allow an I, remote adjusting (X) I a user of an agementation an agementation an agementation an agementation ar agementation ar agementation ar agementation access with a crassful explance attacker acry scription access with a crassful explance attacker acry scription access access with a crassful explance attacker acry scription access	e of (SS) of the ent e to of y the ent che afted loit ser to pt the	N	/A		H-CIS-F 041119	
Improper Neutralizati on of Input	16-	10-2019	3.5	Multiple vulnerabilities in the web-based management interface of			N/A			H-CIS-F 041119		
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3 3-4 4-5 5-6			<u> </u>	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Mana (FMC) auther attack cross-attack web-k interfection web-k interfe	Firepower gement (a) could a conticated for the conticated management (a) against coased management (a) ace. The conticated for the conticated coased management (a) ace to classification the contication (b) coveration. D: CVE-9	Center Illow an , remote nduct a pting (X causer of anageme se s are due ilidation input by anageme attacker these s by user of t ick a cra sful expl ne attack cary scrip ntext of ccess wser-bas	SS) of the ent e to of y the ent he fted oit er to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the web- based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web- based management interface. The vulnerability is due to insufficient validation of				N/A		H-CIS-F 041119	
CV Scoring Scal	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper	Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIF	PC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting') 16-10-2019 3.5 Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit				web-linterficould vulne persuinterfilink. A could execute interfisensity information.	based market ace. An ace exploit erability adding a face to classification the conface or active, brownation.	anagementtacker this by user of the context of the	che afted loit ker to pt				
the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit	firepower_m	anagement_ce	nter_2								
	Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulner insuff userweb-linterf could vulner persuinterf link.	reb-based gement (a) could a centicated where to co-site scrite scrite scrite sagainst based marginal face. The centicated based marginal face and a cexploit or abilitie face to classed t	interfactiver Center Allow an I, remote and I a user of an agementacker an agementacker these as by user of the action of the ac	e of SSS) of the ent e to n of y the ent	N/A			

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	ch	NCIIP	CID
			code interf sensit inform CVE I 1526 Multi the w	ple vuln eb-base	ntext of ccess wser-ba 2019- erabilitie	sed es in				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Cisco Mana (FMC authe attacl cross attacl web-l interf vulne insuff user- web-l interf could vulne persu interf link. A could execu code interf sensit	gement Firepow gement Could a enticated ker to co site scri k against based m face. The ficient va supplied based m face. An a exploit erabilitie face to cl A success allow th the arbit in the co face or a tive, bro mation. D: CVE- 19	cer Center Illow an I, remote Induct a	es (SS) of the ent e to of y the ent the oit cer to pt the	N/A		H-CIS-F 041119	
Improper Neutralizati on of Input	16-10-2019	3.5	A vulnerability in the webbased management interface of Cisco			N/A		H-CIS-F 041119		
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Firepo Cente an un remot condu script agains based interf vulne insuff user-s web-b interf could vulne persu interf link. A could execu code i interf sensit inforr	ower Mar (FMC) authent te attack ict a croing (XSS st a user landing ace. The rability ading a ace to classed mace to classed te arbiting a lace to classed te arbiting ace or a cive, bromation.	anagement could all icated, ser to ss-site S) attacker of the vertical input be anagement attacker this by user of the attacker a	ent llow veb- o of y the ent che afted loit er to pt				
firepower_m	anagement_ce	nter_2	500							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC) authe attack cross- attack web-k	eb-base gement Firepov gement (a) could a nticated ser to co-site scritcians	interfactory ver Center allow an I, remote anduct a ipting (X t a user of anageme	e of (SS) of the	N/A		H-CIS-F 041119	
CV Scoring Sca	le 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	D	escription	1 & CVE II	D	Pato	h	NCIIP	CID
			insuff user-s web-l interf could vulne persu interf link. A could execu code s interf sensit inform	rabilities ficient va supplied based ma face. An a exploit of rabilities face to cla face to cla face to cla face to cla face or ac face or ac face or ac five, brow mation.	input by anagement acker these as by user of the acker ary scriptext of access wser-ba	of y the ent the oit er to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multi the w mana Cisco Mana (FMC authe attack cross- attack web-l interf vulne insuff user web-l interf could vulne persu interf		erabilition d interface ver Center llow an , remote nduct a pting (X a user of anageme s are due input b anageme attacker these s by user of t ick a cra	e of (SS) of the ent e to of y the ent	N/A		H-CIS-F 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	allow th	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE I	D	Pato	:h	NCIIP	CID
			code i interf sensit	te arbitr in the co ace or ac ive, brov	ntext of	the				
			CVE I 1526	D : CVE- 9	2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interf Firepo Cente an un remote conduscript against based interf vulne insuff user-s web-binterf could vulne persuinterf link. A could execu code interf sensit inform	nerability manage ace of Ci authentite attack act a crossing (XSS st a user manage ace. The rability is ace. An acxiding a cased material ace to climate arbitrin the corace or active, brownation. D: CVE-0	ement sco anageme could al cated, er to ss-site) attack of the v ement s due to lidation input b anageme attacker chis by user of t ick a cra sful expl ary scri ntext of ccess wser-ba	ent llow veb- o of y the ent che afted loit er to pt	N/A		H-CIS-F 041119	
firepower_m	anagement_ce	nter_4	000							
Improper Neutralizati	16-10-2019	3.5		ple vulne eb-basec		es in	N/A		H-CIS-F	IRE-
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
on of Input During Web Page Generation ('Cross-site Scripting')			Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execut code interf sensitinform CVE I 1526		Center allow an an are duct a pting (X a user of an agement attacker these as by user of the attack ary scriptext of access weer-bases 2019-	esss) of the ent e to of y the ent the of the ent ser to the ent			041119	/1182
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross attack web-k interf	ple vulne eb-based gement () could a enticated cer to corrict scritcased marked	d interface ver Center illow an , remote nduct a pting (X a user of anagements	e of (SS) of the ent	N/A		H-CIS-F 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			user-s web-k interf could vulne persu interf link. A could execu code i interf sensit inforr	ricient value of supplied based marge. An arcabilities adding a value arbitrate arbitrate arbitrate or active, brown ation. D: CVE-9	input by anagementacker these s by user of the ick a cra sful expl are attack ary scri ntext of ccess wser-ba	y the ent che of the ent cer to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interf Firepo Cente an un remote conduscript against based interf vulne insuff user-s web-binterf could vulne persuinterf link. A could	nerability I manage Tace of Ci ower Ma Tace (FMC) authenti te attack act a cross st a user I manage Tace. The rability i Ticient va supplied based ma Tace. An a exploit to rability l ading a u Tace to cli A success allow th	ement sco inageme could al cated, er to ss-site) attack of the we ement is due to lidation input b anageme attacker this by user of t ick a cra sful expl	ent llow veb- o of y the ent che	N/A		H-CIS-F 041119	
			execu	te arbitr	ary scri	pt				

Weakness	Pu	blish Date	cvss	D	escriptio	n & CVE I	D		Pato	h	NCIIP	CID			
				code	in the co	ntext of	the								
					ace or a										
					tive, bro	wser-ba	sed								
				infori	nation.										
				CVE I	D : CVE-	2019-									
				1527	0										
firesight_man	nage	ment_cer	ter_15	00											
					ple vuln		es in								
					eb-base										
					gement		e of								
					Firepov										
					gement										
				`) could a										
					nticated		2								
				attacker to conduct a cross-site scripting (XSS)											
				attack against a user of the											
				attack against a user of the web-based management											
Improper				web-based management interface. These											
Neutralizati					rabilitie		e to								
on of Input					icient va										
During Web				user-	supplied	l input b	y the				H-CIS-F	IRE-			
Page	16-	10-2019	3.5	web-l	oased m	anagem	ent	N/A	A		041119				
Generation				interf	ace. An a	attacker						•			
('Cross-site				could	exploit	these									
Scripting')				vulne	rabilitie	s by									
				persu	ading a	user of t	he								
					ace to cl										
					A succes	_									
					allow th										
					te arbitı										
					in the co		the								
				interface or access											
				sensitive, browser-based											
				information.											
				CVE ID : CVE-2019- 15268				CVE ID : CVE-2019- 15268							
Improper				Multiple vulnerabilities in							H-CIS-F	IRE-			
Neutralizati	16-	10-2019	3.5	_			N/A			041119					
on of Input				management interface of			<u> </u>								
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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Mana (FMC) auther attack cross-attack web-k interfection web-k interfection web-k interfection with the could execute code interfection web-k interfection with the could execute code interfection web-k interfection with the could execute interfection web-k int	Firepower gement () could a nticated term to consider the script and the supplied pased material trabilities ading a new property of the arbitration of the consider the consideration.	Center Illow an , remote nduct a pting (X a user of anageme s are due ilidation input by anageme attacker these s by user of t ick a cra sful expl ae attack cary scri ntext of ccess wser-ba	esss) of the ent e to of y the ent he ofted oit ter to pt the				
firesignt_mai	nagement_cen	ter_35	1							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These				N/A		H-CIS-F 041119	
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	D	escription	1 & CVE II	D	Pato	h	NCIIP	CID
			insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268							
					2017					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross- attack web-l interf vulne insuff user-s web-l interf could vulne persu interf link. A	ple vulnereb-based gement in Firepower gement in Could a could	interface ver Center llow an , remote nduct a pting (X a user of anagement input by anagement attacker these s by user of t ick a cra	e of SSS) of the ent e to of y the ent he afted oit	N/A		H-CIS-F 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
firesight ma	nagement_cen	ter 75	execute arbitrary script code in the context of the interface or access sensitive, browser-based information. CVE ID: CVE-2019-15269							
mesignt_mai	magement_een	ter_75	•	ple vuln	erabiliti	es in				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulner insuff user-web-linterf could vulner persuinterf link. A could execut code interf sensitinform	reb-based gement (a) could a c	interface ver Center Illow an , remote nduct a pting (X a user of anagement input be anagement input be anagement input be anagement input be anagement input be anagement input be anagement input be anagement attacker these is by user of t ick a crassful explanation for a crassful explanation intext of ccess wser-ba	e of ESS) of the ent of y the ent the afted oit cer to pt the	N/A		H-CIS-F 041119	
Improper Neutralizati	16-10-2019	3.5	Multiple vulnerabilities in the web-based				N/A		H-CIS-F	IRE-
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	Descri	ption & CVE II	D	Pato	h	NCIIP	C ID
on of Input During Web Page Generation ('Cross-site Scripting')			management Cisco Fire Management (FMC) could authenticate attacker to cross-site attack again web-based interface. Vulnerabili insufficient user-supp web-based interface. Could exployulnerabili persuading interface to link. A succould allow execute an code in the interface of sensitive, information	ent interface power ent Center ald allow an ated, remote conduct a scripting (X inst a user of d manageme at validation alied input by d manageme An attacker loit these lities by g a user of t co click a cra cessful expl w the attack bitrary scrip e context of or access browser-base	e of SS) of the ent e to of y the ent he fted oit er to pt the			041119	
sf250-24					l				
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability			N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			prote based interfedevice explosed by pethe immalice succes allow perfowith the tauser leprivile could configure comments on denial conditions.	D : CVE-	or the weement on affected acker coolinerability a user of followers. A coloit country actility actility actility attacked attacked action (DoS) an affect	eb- ed uld lity of a ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack	nerability I interface Busines ged Switty an unaute attack act a crost aing (XSS) st a user I interface rability in ficient value based interface actions acti	ce of Cisons Smart teches continued to see to see to see the work of the work of the total idation alignment between the centre of the centre of the terface of the work of the terface of the centre of the terface of the te	and uld ated, veb-	N/A		H-CIS-S 041119	
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

persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718 A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches 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 for the web-based management interface of on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of	Weakness	Publish Date	CVSS	De	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches 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 for the web- based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of				malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-							
Cross-Site Request Forgery (CSRF) 16-10-2019 6.8 based management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of	sf250-24p										
the targeted user. If the	Request Forgery	16-10-2019	6.8	based interfar Busin Managallow remote conducting attack system is due protect based interfar device exploit by performalicity success allow performation with the success and the success allow performation with the success and the success	manage ace of Ciess Smaged Swiran unaute attack across forge and an amage ace on a ace. An attack ace on a ace attack ace on a ace on a ace attack ace on a ace ace on a ace attack ace on a ace attack ace on a ace ace on a ace ace ace attack ace on a ace on a ace ace on a ace ace on a ace ace on a ace ace ace ace ace ace ace ace ace a	ement isco Sma rt and tches co ithentica ier to iss-site ry (CSRI iffected ulnerab ifficient (or the we ement in affecte acker co ilnerabi g a user to follow is. A bloit cou cker to crary act lege leve	uld ated, ility CSRF eb- ed uld lity of a ld ions el of	N/A			

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SF25- 041119/1194

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sf250-48					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SF25- 041119/1195
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SF25- 041119/1196
on of Input			Small Business Smart and		
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
During Web Page Generation ('Cross-site Scripting')			Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	racii	
sf250-48hp					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability	N/A	H-CIS-SF25- 041119/1197
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pat	ch	NCIIP	CID
			prote based interfedevice explosed by pethe immalice succes allow perfowith the tauser leprivile could configure comments on denial conditions.	D : CVE-	or the weement in affected acker coulinerability a user of following a country activity activity attacked attacked activity activity activity attacked activity activity activity attacked activity activity attacked activity activity attacked activity activity activity attacked activity activity attacked activity activity attacked activity activ	eb- ed ould lity of ld ions el of ne er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by				N/A		H-CIS-S 041119	
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg250-08					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG25- 041119/1199

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG25- 041119/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg250-08hp					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG25- 041119/1201
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SG25- 041119/1202
on of Input			Small Business Smart and		
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	C	Description & CVE ID			Pato	:h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Mana allow remo condiscrip again based vulne insuffect attack vulne persuinter; malic subset speci page. could execu code affect acces based CVE	Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718						
sg250-10p										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability			N/A		H-CIS-SG25- 041119/1203		
CV Scoring Sca	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	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
			prote based interfedevice explosing the immalice succes allow perfosith the tauser light could configure comments on the condition of the could configure comments on the could configure condition of the could configure condition of the could condition of the condition	D : CVE-	or the weement in affected acker coulinerability a user of following a country actility actility attacked attacked action (DoS an affect	eb- ed uld lity of ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack	nerability I interface Busines ged Switty an unaute attack act a crost acting (XSS) st a user I interface rability in ficient value based interface actions ac	ce of Cisons Smart teches continued to see to see the work of the work of the total idation alidation terface of the ce. An all exploits	and uld ated, veb-	N/A		H-CIS-S 041119	
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg250-18					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG25- 041119/1205

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG25- 041119/1206

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg250-26					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG25- 041119/1207
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SG25- 041119/1208
on of Input			Small Business Smart and		
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	Descriptio	n & CVE ID		Pato	:h	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')			Managed Swi allow an unau remote attack conduct a croscripting (XSS against a user based interfactular vulnerability insufficient vauser-supplied web-based in affected device attacker could vulnerability persuading a interface to chemalicious link subsequently specific web it page. A succe could allow the execute arbitic code in the coaffected interfaces sensiti based inform CVE ID: CVE 12718	tches counthenticater to ass-site (S) attack of the work. The is due to alidation dinput by terface of the work and access a anterface ssful exploit extack of the attack	eb- of the fthe this ne				
sg250-26hp					L				
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability			N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pate	:h	NCIIP	CID
			prote based interfedevice explosed by performation with the tauser light could configure comments of the condition of the condition of the condition of the could configure comments of the condition of the condi	D : CVE-	or the weement in affected acker coulinerability a user of following a country actility actility attacked attacked action (DoSan affective).	eb- ed uld lity of a ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack	nerability I interface Busines ged Swite an unaute attack uct a crost cing (XSS st a user I interface rability in contact device wer could crability in	ce of Cisons Smart teches continued to see to see to see the work of the work of the total idation alignment between the centre of the centre of the terface of the work of the terface of the centre of the terface of the te	and uld ated, veb-	N/A		H-CIS-S 041119	
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg250-26p					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG25- 041119/1211

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG25- 041119/1212

sg250-50 Cross-Site Request Forgery (CSRF)			A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could		
Cross-Site Request Forgery			based management interface of Cisco Small Business Smart and Managed Switches 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 for the web- based management interface on an affected		
Request Forgery			based management interface of Cisco Small Business Smart and Managed Switches 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 for the web- based management interface on an affected		
	-10-2019	6.8	device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG25- 041119/1213
Improper Neutralizati 16-	-10-2019	4.3	A vulnerability in the webbased interface of Cisco	N/A	H-CIS-SG25-
on of Input	・エロームロエフ		Small Business Smart and	,	041119/1214

Weakness	Publish Date	CVSS	Description	& CVE ID	Pate	ch	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')			Managed Switch allow an unauth remote attacker conduct a cross scripting (XSS) against a user based interface vulnerability is insufficient valuser-supplied web-based interfaced device attacker could vulnerability be persuading a uninterface to climalicious link subsequently a specific web in page. A success could allow the execute arbitrate code in the coraffected interfaces sensitive based informatic CVE ID: CVE-2718	ches could thenticated, er to es-site) attack of the web- e. The s due to lidation of input by the erface of the e. An exploit this by user of the ck a and access a aterface sful exploit e attacker to ary script attack of the ace or re browser- tion.				
sg250-50hp					•			
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability based manager interface of Cis Business Smar Managed Swite allow an unaut remote attacker conduct a cross request forger attack on an af system. The vulnerable system.	N/A		H-CIS-S 041119		
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			prote based interfedevice explosing the immalice succes allow perfosith the tauser light could configure comments on the condition of the could configure comments on the could configure condition of the could configure condition of the could condition of the condition	D : CVE-	or the weement in affected acker coulinerability a user of following a country actility actility attacked attacked action (DoS an affect	eb- ed uld lity of ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack	nerability I interface Busines ged Switty an unaute attack act a crost aing (XSS) st a user I interface rability in ficient value based interface and device arability in ficient value and device arability in ficient value arability in	ce of Cisons Smart teches continued to see to see the work of the work of the total idation alidation terface of the ce. An all exploits	and uld ated, veb-	N/A		H-CIS-S 041119	
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg250-50p					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG25- 041119/1217

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG25- 041119/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg250x-24					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG25- 041119/1219
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SG25- 041119/1220
on of Input			Small Business Smart and		011117/1220
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		escriptio	n & CVE I	D	Pato	h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Mana allow remote cond scrip again based vulne insuffect attact vulne persuinter malic subset special page. could execut code affect access based CVE	allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718						
sg250x-24p										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability			N/A		H-CIS-S 041119		
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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			prote based interfedevice explosing the immalice succes allow perfosith the tauser light could configure comments on the condition of the could configure comments on the could configure condition of the could configure condition of the could condition of the condition	D : CVE-	or the weement in affected acker coulinerability a user of following a country actility actility attacked attacked action (DoS an affect	eb- ed uld lity of ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by			N/A		H-CIS-S 041119		
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg250x-48					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG25- 041119/1223

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG25- 041119/1224

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg250x-48p					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG25- 041119/1225
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SG25- 041119/1226
on of Input			Small Business Smart and		
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
During Web Page Generation ('Cross-site Scripting')			Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718		
sf350-08					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability	N/A	H-CIS-SF35- 041119/1227
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			prote based interfedevice explosed by performation with the tauser light could configure comments of the condition of the condition of the condition of the could configure comments of the condition of the condi	D : CVE-	or the weement on affected acker coolinerability as user of following a user of the country activity activity attacked activity activity activity activity attacked activity a	eb- ed uld lity of a ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by			N/A		H-CIS-S 041119		
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718							
sf350-24										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interf Busin Mana allow remove condureque attack system is due prote based interf device explo by perturbation malicular succe allow perfor with the succession of the interference	nerabilited manage ace of Commerce of Commerce are attacked at a cross forger and a commerce on a co	ement asco Sma rt and tches co athentica er to ass-site ry (CSRI affected ulnerab fficient (or the we ement n affecte acker co alnerabi g a user to follow c. A bloit cou cker to crary act lege lev	all uld ated, ility CSRF eb- ed ould lity of a ild ions el of	N/A		H-CIS-S 041119	
	ale 0.4									

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SF35- 041119/1230

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sf350-24mp					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SF35- 041119/1231
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SF35- 041119/1232
on of Input	<u> </u>		Small Business Smart and		, , , , , , , , , , , , , , , , , , , ,
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		Pato	h	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')			Managed Swit allow an unauremote attacker conduct a cross scripting (XSS) against a user based interfact vulnerability insufficient valuser-supplied web-based interfacted device attacker could vulnerability be persuading a uninterface to climalicious link subsequently a specific web in page. A success could allow the execute arbitracede in the condification of the condition of	ches could thenticated er to ss-site) attack of the web e. The s due to lidation of input by the erface of the exploit this by user of the eck a and access a aterface esful exploit e attacker that ary script exploit ary script extent of the face or we browser attion.	t to				
sf350-24p									
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability based manage interface of Cis Business Smar Managed Swit allow an unauremote attacked conduct a cross request forger attack on an all system. The vu	d,	N/A		H-CIS-S 041119		
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5 5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			prote based interf device explose the immalic succe allow perfo with the tauser herivil could configure communication device CVE I	D : CVE-	er the weement in affected acker coulinerability as user of following a country activity activity attacked activity acti	eb- ed uld lity of ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this			N/A		H-CIS-S 041119	
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	De	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
			interfamalici subse specif page. could execu code i affecte access based	ace to clious link quently ic web i A succe allow th te arbite n the co ed inter s sensiti inform D: CVE	and access anterface ssful exp ne attack ary scri ontext of face or ve brow ation.	oloit eer to pt				
sf350-48										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interface Busin Managallow remote conducting attack system is due protection by performalicing successible allow perfor with the successible attack system is due to be a sed interface and the successible attack system in the interface of	manage ace of Control ess Smanged Swinger and unaute attacked across forger ace on a manage ac	rt and rt and tches co athentica ter to ss-site ry (CSRI affected ulnerab fficient (or the we ement n affecte acker co alnerabi g a user to follow x. A ploit cou	all uld ated, ility CSRF eb- ed ould lity of a ild ions el of	N/A		H-CIS-S 041119	
CV Scoring Sca	ole 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
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SF35- 041119/1236

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			12718					
sf350-48mp								
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SF35- 041119/1237			
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SF35- 041119/1238			
on of Input			Small Business Smart and					
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	C	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Mana allow remo condiscrip again based vulne insuffect attack vulne intermalic subset specipage. could executed affect access based	aged Swi van unau ite attack uct a cro ting (XSS ast a user d interface erability ficient va supplied based in ted device ker could erability nading a face to classified equently fic web i A succe I allow that in the could ted interface in the could ted interface ted interface t	tches conthenticater to ss-site S) attack of the voce. The didation of the voce and access a cand access a cary scripping attack of face or ve brown attion.	uld ated, eveb- or of the of the che che che che che che che che che c			NCIII*	
sf350-48p										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based internations Busin Mana allow remo condi- reque attack	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability					H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			prote based interf device explo by per the in malic succe allow perform with the tauser had configured configured condition device CVE I	D : CVE-	er the weement on affected acker coolinerability as user of followers. A coloit country activities attacked attacked activities attacked activitie	eb- ed uld lity of ld lions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by			N/A		H-CIS-S 041119		
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	Desc	riptior	a & CVE I	D	Pato	:h	NCIIP	C ID
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718							
sf352-08			12,10							
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulner based m interface allow an remote a conduct request attack or system. I is due to protection based m interface device. A exploit to by persure the intermalicious successful allow the perform with the target.	anage e of Cis s Smar d Swit n unau attack a cros forger n an as The vo insuf ons fo anage e on ar An atta chis vu uading rface t us link ful exp e attac a crbiti e privil	ement sco Sma rt and ches co thentica er to ss-site ry (CSRI ffected ulnerab fficient (r the we ement n affecte acker co alnerabi g a user o follow A bloit cou cker to rary act lege leve	uld ated, ility CSRF ed ould lity of a ild ions el of	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SF35- 041119/1242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sf352-08mp					<u> </u>
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SF35- 041119/1243
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco	N/A	H-CIS-SF35- 041119/1244
on of Input			Small Business Smart and		,
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 754	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE	ID	Pato	:h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Managed Switches coallow an unauthentice remote attacker to conduct a cross-site scripting (XSS) attack against a user of the based interface. The vulnerability is due to insufficient validation user-supplied input loweb-based interface affected device. An attacker could exploit vulnerability by persuading a user of interface to click a malicious link and subsequently access specific web interface page. A successful excould allow the attack execute arbitrary scription code in the context of affected interface or access sensitive brow based information. CVE ID: CVE-2019-12718	ould rated, or web- on of oy the of the this the a e ploit ker to ipt f the				
sf352-08p				•				
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the based management interface of Cisco Sm Business Smart and Managed Switches coallow an unauthentic remote attacker to conduct a cross-site request forgery (CSR attack on an affected system. The vulneral	all ould rated, F)	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
			prote based interfedevice explosing the immalice succes allow perfosith the tauser in the privile could configure comments on the could configure the could configure comments on the could configure could could configure could configure could configure could configure country could configure co	D : CVE-	or the weement on affected acker coolinerability as user of following a user of the country activity activity attacked attacked activity activity attacked activity a	eb- ed uld lity of a ld lons el of ne ve or				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this			N/A		H-CIS-S 041119	
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg350-10					
Cross-Site Request Forgery (CSRF)	S-Site lest ery F) 16-10-2019 6.8 A vulubased internation allow remote conduration system is due protein the remote conduration in the remote conduration attacks system is due protein the remote conduration in the remote conduction attacks and requirements at a conduction attacks and remote conduction attacks and remote conduction attacks at a conduction attacks and remote conduction attacks and remote conduction attacks and remote conduction attacks and remote conduction attacks are also attacks and remote conduction attacks are also attacks and remote conduction attacks are also attacks and remote conduction attacks and remote conduction attacks are also attacks and rem		A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG35- 041119/1247

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG35- 041119/1248

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg350-10mp					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG35- 041119/1249
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SG35- 041119/1250
on of Input			Small Business Smart and		
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	C	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')			Mana allow remo condiscrip again based vulne insuffect attack vulne intermalic subset specipage. could executed affect access based	ged Swi an unaute attack uct a cro ting (XSS st a user d interfact erability ficient value based in ted device ker could rability adding a face to claious link equently fic web i A succe allow that the arbita in the could the arbita the arbita in the could the arbita the arbita the arbita the arbita the could the arbita the arbita	tches conthenticater to ss-site (S) attack of the voce. The didation of the voce and dexploit by user of the voce and access access and access access access and access a	uld ated, web- on of oy the of the this the coloit ser to opt the of the of the other than the o				
sg350-10p										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability			N/A		H-CIS-S 041119		
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			prote based interfedevice explosed by performalice succes allow perform with the tauser less that the tauser less commended conditions and interfedevice the conditions of the	D : CVE-	or the weement in affected acker coulinerability a user of following a country active active attacked attacked active (DoS) an affect	eb- ed uld lity of ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by			N/A		H-CIS-S 041119		
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg350-10sfp					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG35- 041119/1253

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG35- 041119/1254

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg350-20					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG35- 041119/1255
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SG35- 041119/1256
on of Input			Small Business Smart and		
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
During Web Page Generation ('Cross-site Scripting')			Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718		
sg350-28					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability	N/A	H-CIS-SG35- 041119/1257
CV Scoring Sca	le 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	·				Pato	ch	NCIIP	CID
			prote based interfedevice explosed by performalic succes allow perform with the tauser less that the tauser less comments of the tauser less comments conditions and the tauser less than the tauser l	D : CVE-	er the weement in affecte acker co alnerabil g a user of to follow a. A bloit cou cker to rary acti lege leve aser. If the nistrativ e attacke a execute c cause a fice (DoS an affect	eb- ed uld lity of ld lons el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by			N/A		H-CIS-S 041119		
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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg350-28mp					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the	N/A	H-CIS-SG35- 041119/1259

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG35- 041119/1260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg350-28p					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG35- 041119/1261
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SG35- 041119/1262
on of Input			Small Business Smart and		
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
During Web Page Generation ('Cross-site Scripting')	rubiisii Date	CV33	Mana allow remo conditions again based vulner affect attack vulner malic subset speci page. could execu code affect acces based	ged Swi an unaute attack uct a cro ting (XSS st a user d interfact erability ficient value based in ted device ker could rability adding a face to claious link equently fic web it A succe allow that in the could ted interfact in the could ted interfact serious link equently fic web it allow that in the could ted interfact in the could ted interfact ted interfact in the could ted interfact ted interfa	tches conthenticater to ss-site (S) attack of the voce. The didation of the voce and dexploit by user of the voce and access access and access and access access and access and access access and access access and access access access and access access access access and access	uld ated, eveb- of of the of the character to pt the of th	Patt		INCHIP	CID
sg350-28sfp										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability				N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
			prote based interfedevice explosing the immalice succes allow perfosith the tauser light could configure comments on the condition of the could configure comments on the could configure condition of the could configure condition of the could condition of the condi	D : CVE-	or the weement in affected acker coulinerability a user of following a country actility actility attacked attacked action (DoSan affective).	eb- ed uld lity of a ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by				N/A		H-CIS-S 041119	
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	De	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
			interfa malici subsect specifi page. A could execut code it affecte access based	ace to clous link quently ic web it A succest allow the te arbite on the content is sensitition information.	and access anterface ssful exp ne attack ary scri ontext of face or ve brow ation.	oloit eer to pt the				
sg350-52										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interfate Busine Managallow remote conduratack system is due protect based interfate device exploit by perthe interfate based interfate device exploit by perthe interfate based interfate by perthe interfate by performalicity with the performance of the performance	manage ace of Ciess Smaged Switan unaute attacked to crost forge on an actions for manage ace on actions for action	rt and rt and tches co athentica er to ss-site ry (CSRI affected ulnerab fficient (or the we ement n affecte acker co alnerabi g a user to follow c. A ploit cou	uld ated, ility CSRF eb- ed ould lity of a ild ions el of	N/A		H-CIS-S 041119	

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG35- 041119/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg350-52mp					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG35- 041119/1267
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco	N/A	H-CIS-SG35- 041119/1268
on of Input			Small Business Smart and		011117/1200
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	n & CVE ID		Pato	h	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')			Managed Switt allow an unauremote attack conduct a crosscripting (XSS against a user based interface vulnerability insufficient vauser-supplied web-based interface device attacker could vulnerability in persuading a interface to climalicious link subsequently specific web in page. A success could allow the execute arbitricode in the coaffected interfaces sensitive based informatic CVE ID: CVE-12718	tches could athenticate ter to ass-site so attack of the webe. The distriction of a input by the terface of the terface of the terface of the terface of the terface attacker ary script acceptance of the face or we browser ation.	d, f he he his it to e				
sg350-52p									
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability based manage interface of Ci Business Smar Managed Swit allow an unau remote attack conduct a cross request forger attack on an a system. The version of the system of t	l d,	N/A		H-CIS-S 041119		
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			prote based interfedevice explosed by performalic succes allow perform with the tauser less that the tauser less comments of the tauser less comments conditions and the tauser less than the tauser l	D : CVE-	or the weement in affected acker coulinerability a user of following a country active active attacked attacked active (DoS) an affect	eb- ed uld lity of ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by				N/A		H-CIS-S 041119	
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	De	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
			interfa malici subsecti specifi page. A could execut code i affecte access based	ace to clous link quently ic web it A succestallow the tearbite on the content is sensition information.	and access anterface ssful exp ne attack ary scri ontext of face or ve brow ation.	oloit eer to pt the				
sg350-8pd										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interfate Busine Managallow remote conductive attack system is due protect based interfate devices exploit by per the interfate allow perfor with the conductive and the conductive allow perfor with the conductive and the conductive allow perfor with the conductive and the	manage ace of Control ess Smarged Swinger artacker across forger and an ace on a control est this vertical essential experience of the attacker arbit the attacker arbit he priving ace on a control essential experience of the attacker arbit arbit he priving ace on a control essential experience of the attacker arbit arbit he priving ace on a control essential experience acceptance of the attacker arbit arb	rt and rt and tches co athentica ter to ss-site ry (CSRI affected ulnerab fficient (or the we ement n affecte acker co alnerabi g a user to follow x. A ploit cou	uld ated, ility CSRF eb- ed ould lity of a ld ions el of	N/A		H-CIS-S 041119	

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SG35- 041119/1272

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg355-10p					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SG35- 041119/1273
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco	N/A	H-CIS-SG35- 041119/1274
on of Input			Small Business Smart and		011117/12/4
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
During Web Page Generation ('Cross-site Scripting')			Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718		
sf550x-24					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability	N/A	H-CIS-SF55- 041119/1275
CV Scoring Sca	le 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	D	escription	ո & CVE II	D	Pato	ch	NCIIP	CID
			prote based interfedevice explosed by performalic succes allow perform with the tauser less that the tauser less comments of the tauser less comments conditions and the tauser less than the tauser l	D : CVE-	er the weement in affecte acker co alnerabil g a user of to follow a. A bloit cou cker to rary acti lege leve aser. If the nistrativ e attacke a execute c cause a fice (DoS an affect	eb- ed uld lity of ld lons el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack	nerability I interface Busines ged Swite an unaute attack uct a crost cing (XSS st a user I interface rability in ficient va supplied based interface crability in the device could crability in	te of Ciscons Smart ches contithenticater to ss-site of the way the ce. The didation input by terface of the ce. An didation the ce.	and uld ated, web-	N/A		H-CIS-S 041119	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Forgery (CSRF) 6.8 protections for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions	interface to click a malicious link and subsequently access a specific web interface page. 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- 12718 A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches 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 for the web- based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to	Weakness	Publish Date	CVSS	De	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Cross-Site Request Forgery (CSRF) 16-10-2019 6.8 A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions	based management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to				interfamalications interfamalications in the malication in the mal	ace to clious link quently ic web i A succe allow th te arbita in the co ed inter s sensiti informa D: CVE	ick a and access a nterface ssful exp e attack cary scri ontext of face or ve brow ation.	oloit er to pt the				
Cross-Site Request Forgery (CSRF) 16-10-2019 6.8 based management interface of Cisco Small Business Smart and Managed Switches 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 for the web- based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions	based management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to	sf550x-24mp)									
the targeted user. If the	with the privilege level of	Request Forgery	16-10-2019	6.8	based interface Busin Managallow remote attack system is due protection by performalicing successible allow perforwith to the system of the interface and the system of the interface attack system is due to the interface attack and the system of the interface attack and the system of the interface attack and the system of t	manage ace of Ciess Smaged Switan unaute attack act a crost forge and an amage ace on a ce. An attack ace on a ce. An attack act a crost forge ace on a ce. An attack attack attack attack act	ement isco Sma rt and tches co ithentica ter to ss-site ry (CSRI iffected ulnerab ifficient (or the we ement in affecte acker co ulnerabi g a user to follow k. A ploit cou cker to crary act lege leve	all uld ated, ility CSRF eb- ed ould lity of a ild ions el of	N/A			

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SF55- 041119/1278

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sf550x-24p					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SF55- 041119/1279
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SF55- 041119/1280
on of Input			Small Business Smart and		
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	Pato	ch	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')			Managed Switch allow an unauth remote attacker conduct a cross scripting (XSS) against a user of based interface vulnerability is insufficient valid user-supplied in web-based interface attacker could evulnerability by persuading a uninterface to click malicious link a subsequently a specific web into page. A success could allow the execute arbitraticode in the condiffected interface access sensitive based informaticode in the condition of the	ches could henticated, or to s-site attack of the web- c. The due to idation of nput by the erface of the . An exploit this y ser of the ck a and ccess a terface oful exploit e attacker to ary script text of the ice or e browser- cion.				
sf550x-48								
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability based manager interface of Cisc Business Smart Managed Switc allow an unaut remote attacke conduct a cross request forgery attack on an aff system. The vulneral conduct with the system of the syst	ment co Small t and ches could henticated, or to s-site y (CSRF)	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
			prote based interfedevice explosing the immalice succes allow perfosith the tauser light could configure comments on the condition of the could configure comments on the could configure condition of the could configure condition of the could condition of the condi	D : CVE-	or the weement on affected acker coolinerability as user of following a user of the country activity activity attacked activity activity activity activity attacked activity a	eb- ed uld lity of a ld ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack	nerability I interface Busines ged Swite an unau te attack act a crost cing (XSS st a user I interface rability in ficient va supplied based interface ced device cer coulce crability in	ce of Cisons Smart ches continued to ss-site of the way to allidation input by terface of the ce. An dexploit	and uld ated, veb-	N/A		H-CIS-S 041119	
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	Des	cription	n & CVE I	D	Pato	:h	NCIIP	C ID
			malicion subseque specific page. A could all execute code in affected access subased in CVE ID	interface to click a malicious link and subsequently access a specific web interface page. 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- 12718		Patch N/A				
sf550x-48mp			12/10							
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulne based minterface Business Manage allow ar remote conduct request attack of system. Is due to protectif based minterface device. A exploit of by person the intermalicious successivallow the perform with the target.	nanage e of Ci es Smar ed Swit n unau attack t a cros forger on an a The vi o insuf ions fo nanage e on a this vu uading rface t us link ful exp ne attac n arbit e privi	ement sco Sma rt and ches co thentica er to ss-site ry (CSRI ffected ulnerab fficient (or the we ement n affecte acker co alnerabi g a user to follow cker to rary act lege lev	all uld ated, ility CSRF eb- ed ould lity of a ild ions el of	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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
			user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	H-CIS-SF55- 041119/1284

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12718		
sf550x-48p					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SF55- 041119/1285
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SF55- 041119/1286
on of Input			Small Business Smart and		,
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
During Web Page Generation ('Cross-site Scripting')			Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
spa122					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to conduct cross-site scripting attacks. The vulnerability is due to insufficient validation of	N/A	H-CIS-SPA1- 041119/1287
CV Scoring Sca	le 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	D	escription	a & CVE II	D	Pato	h	NCIIP	C ID
			web-binterfisoftware could vulner persuare craft explorate context interfisensit inform	supplied based mare. An are. An are. An are exploit trability bading a uted link. It could are to exercise or acceptance or acceptance or acceptance or acceptance. D: CVE-2	anagement affects this by user to compare allow the ecute because affected affected weeks where because where we have a success where because where a success where because where a success where because a success where a success where because a success where because a success where because a success where a success which is a success where a success which we success which is a success	ent ed click ssful e n the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	2.9	based interface ATA vector could unaut attack site so vulne insuff user-software could vulne malicinaffecter and the user to A successive allow	nerability and are of the are of the are. An are software of the are the attached by the are the attached by the attached	ement sco SPA ter Devi ed, adja nduct cr attacks. s due to lidation input by anageme e affecte attacker this by sendi ut to the rare thro requests uading a crafted xploit co cker to	122 ices cent ross- The of y the ent ed ough s, a link. ould	N/A		H-CIS-S: 041119	
			execu	te arbitr	ary scri	pt				

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
			affect acces based CVE I 1270		face or ve, browation. •2019-	/ser-				
Information Exposure	16-10-2019	4	based interf Series Adap allow remo the confiles of the wind attack web-linterf device exploattack on the result of series.	nerability I manage face of Cr s Analog ters (AT an auth te attack on an aff culnerab oper inp e web-ba gement ker could reque based m face of an e. A succe it could ker to re cuts of ar e device ting in the asitive in D: CVE- 4	ement asco SPA Telepho As) coul enticate er to vie of arbitra ected de ility is d ut valida sed interface d exploit by sendi st to the anagemon affecte essful allow th trieve th bitrary possibl ne disclo aformati	100 one d d, ew ary evice. ue to ation e. An ethis ing a ent d e files y sure	N/A		H-CIS-S 041119	
Information Exposure	16-10-2019	4	based interf Series Adap allow	nerabilit I manago Face of Co s Analog ters (AT Fan auth te attack	ement isco SPA Telepho As) coul enticate	100 one d d,	N/A		H-CIS-S 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			sensitive information on an affected device. The vulnerability is due to unsafe handling of user credentials. An attacker could exploit this vulnerability by viewing portions of the web-based management interface of an affected device. A successful exploit could allow the attacker to access administrative credentials and potentially gain elevated privileges by reusing stolen credentials on the affected device. CVE ID: CVE-2019-							
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multi Cisco Analo Adapt allow adjace execut with of The v to impuser-s web-linterf could vulne auther based interf crafter affect						H-CIS-S 041119	
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 D	ate	cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
				with on Note: mana enable CVE I 1524 Multi Cisco Analo	ple vuln SPA100 og Telepl	privilegen bebased interfaction fault. 2019- erabilition Series mone	e is				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-20	19	5.2	allow adjact executive with a to impure web-linterfacture auther based interfacture affect succes allow executive with a total with a total enable.	Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web- based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-					H-CIS-S 041119	
Improper Restriction of	16-10-20	19	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone				N/A		H-CIS-S 041119	
Operations				Adapters (ATAs) could							
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	D	escription	n & CVE II	D	Pate	ch	NCIIP	CID
within the Bounds of a Memory Buffer			adjace execution with a to impuser-structure interfection of the could will based interfection at the affect succe allow execution with a total with a total enable.	an authorite arbitrelevated ulnerabited based made. An an exploited rabilities of accent and ed requested devices ful expetite arbitrelevated. The well gement ed by de D: CVE-2	eker to rary code privileg ilities are ralidation input to anagement sending sts to an ee. A cloit coucker to rary code privileg to-based interface fault.	e ges. e due n of o the ent web-				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-				N/A		H-CIS-S 041119	
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
			based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019- 15243		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default.	N/A	H-CIS-SPA1- 041119/1295

5-6

6-7

7-8

8-9

9-10

3-4

1-2

0-1

2-3

CV Scoring Scale

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019- 15244		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-	N/A	H-CIS-SPA1- 041119/1296
			15245		
Improper Restriction of Operations within the Bounds of a Memory Buffer	crations erations thin the unds of a mory ffer Cisco SPA100 Series Analog Telephone Adapters (ATAs) coallow an authentical adjacent attacker to execute arbitrary cowith elevated privileges.		Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due	N/A	H-CIS-SPA1- 041119/1297

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pato	h	NCIIP	CID
			to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-							
					2019-					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapt allow adjace execu with execu with execu to impuser-s web-binterf could vulne authe based interf crafte	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A					H-CIS-S 041119	
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	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID				
			executivith of Note: mana enabl CVE I 1524	ple vuln	rary cod privilego-based interfactofault. 2019-	ges. e is								
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Analogallow adjact execution with a to impuse of the could will be auther based interference allow execution with a to impuse of the could will be a to impuse of the could with a to impuse of the could be a to impuse of	Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web- based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-					H-CIS-S 041119					
Improper Restriction of	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone				Cisco SPA100 Series N/A					H-CIS-SPA1- 041119/1300		
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
Operations within the Bounds of a Memory Buffer			Adapta allow adjace execution with a to impuse result web-linterficuld vulne auther based interficrafte affect succe allow execution with a total with a total result	ters (ATA an author ent attace te arbitre elevated ulnerabit proper v supplied based ma ace. An a exploit i rabilities nticating manage ace and ed reques ed devic ssful exp the atta te arbitre elevated The wel gement ed by de D: CVE-	As) could enticate clear to cary code privileg alidation anagement sending sts to an eloit could clear to cary code privilegobased interface fault.	d d, e ees. e due n of o the ent ld ees.				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by				N/A		H-CIS-S 041119	
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
			authenticating to the webbased management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15250		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is	N/A	H-CIS-SPA1- 041119/1302

Weakness	Pul	blish Date	e CVSS	D	escriptio	n & CVE I	D		Pato	h	NCIIP	C ID
				enabl	led by de	fault.						
				CVE I 1525	ID : CVE- 31	2019-						
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-	10-2019	5.2	Cisco Analo Adap allow adjac execu with The v to im user- web- interf could vulne auther based interf crafte affect succe allow execu with Note: mana enabl	ple vuln SPA100 og Telepl ters (AT an auth ent attac te arbite elevated proper v supplied based m face. An a l exploit erabilitie enticatin d manage face and ed reque ted device essful exp the atta te arbite elevated the atta te arbite elevated the atta te levated the atta te arbite elevated the atta the well the well the by de the	Series hone As) coul enticate cker to cary cod privileg ilities are validatio linput to anagement sending sts to an exert course to cary cod privileg b-based interfacted.	d d, e ges. e due n of o the ent dld e ges.	N/	'A		H-CIS-S 041119	
Information Exposure	16-	10-2019	4	A vulnerability in the web- based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on				N/	'A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	3-4	4-5	4-5 5-6		6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			vulne impro config An att this v sendi affect the w mana succe allow return config that c sensit	ected de rability is per rest guration tacker coulnerabing a requed device bebased gement is sful expanding artion ould also tive information	s due to rictions information describing the strong describing information.	on ation. loit n gh e. A ld				
				D : CVE- 7	2019-					
Improper Input Validation	16-10-2019	6.8	based interf Series Adapt allow remore denia on an vulne improusers the wind mana attack vulne crafte web-kinterf device explo	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper validation of user-supplied requests to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to cause the					H-CIS-S 041119	
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
			requiring manual intervention for recovery. CVE ID: CVE-2019- 15258		
sf200-24					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	N/A	H-CIS-SF20- 041119/1306
sf200-24fp					
Improper Neutralizati	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco	N/A	H-CIS-SF20- 041119/1307
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	Patc	h	NCIIP	C ID
on of Input During Web Page Generation ('Cross-site Scripting')			Small Business Smart and Managed Switches 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 device. An attacker could exploit the vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker execute arbitrary script code in the context of the affected interface or access sensitive browses based information. CVE ID: CVE-2019-12718	nd d ed, b- of the the his e			
sf200-24p							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the way based interface of Cisco Small Business Smart are Managed Switches could allow an unauthenticate remote attacker to conduct a cross-site scripting (XSS) attack against a user of the we based interface. The	nd d ed, N/A		H-CIS-S 041119	
CV Scoring Sca	le 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
			vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the	N/A	H-CIS-SF20- 041119/1309

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sf200-48p					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the webbased interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	N/A	H-CIS-SF20- 041119/1310

Weakness	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pat	tch	NCIIP	C ID
				affected interface or access sensitive browserbased information. CVE ID: CVE-2019-							
				1271		2019-					
sf200e-24											
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability and under the attack act a croating (XSS st a user linterfactorability and act a could based interfactorability adding a face to claim and act a could be attack and a country fic web in the country and act are arbitring the country and act arbitring a face to claim and act arbitring and act arbitring and act arbitring act arbitring and act arbitring act arbitring and act arbitring	ce of Cisc is Smart itches co athentica iter to iss-site of the v ce. The is due to alidation input b terface of te. An d exploit by user of t ick a access a nterface ssful exp access a nterface is attack access a nterface of access a nterface or ve brow ation.	co and uld ated, veb- of the this che coloit ser to pt the	N/A		H-CIS-S 041119	
sf200e-24p Improper	16-	10-2019	4.3	A 1711	nerabilit	w in the	woh	N/A		H-CIS-S	F20
CV Scoring Sca									7.0		
(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	Pato	ch	NCIIPC ID
Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')			based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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- 12718			041119/1312
sf200e-48						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-	N/A		H-CIS-SF20- 041119/1313
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-1	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			based interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718							
sf200e-48p			12/1							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack	nerability I interfact Busines ged Swi an unau te attack uct a cro ting (XSS st a user d interfact erability ficient va supplied based in ted device erability	ce of Ciscos Smart tches conthenticater to ss-site of the voce. The didational input beterface of the control input beterfac	and uld ated, web-	N/A		H-CIS-S 041119	_		
CV Scoring Sca	le 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
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg200-08					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script	N/A	H-CIS-SG20- 041119/1315

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

code in the context of the affected interface or access sensitive browser-based information. CVE ID: CVE-2019-12718 A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface to click a malicious link and subsequently access a specific web interface to 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-2019-12718	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') 16-10-2019 A.3 4.3 4.3 H-CIS-SG20- 041119/1316 H-CIS-SG20- 041119/1316 H-CIS-SG20- 041119/1316	sg200-08p			affected interface or access sensitive browserbased information. CVE ID: CVE-2019-		
00°11111 1114m	Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-	N/A	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	N/A	H-CIS-SG20- 041119/1317
sg200-18					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack	N/A	H-CIS-SG20- 041119/1318
CV Scoring Sca (CVSS)	ole 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
			against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718		
sg200-26					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this	N/A	H-CIS-SG20- 041119/1319

2-3

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-13718							
sg200-26fp			1271	8						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit				N/A		H-CIS-S 041119	
CV Scoring Sca	le 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
			execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
sg200-26p					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	N/A	H-CIS-SG20- 041119/1321

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	CID
sg200-50										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	Mana allow remo conduscript again based vulne insuff user-web-laffect attack vulne persuinterf malic subset specific page. could execut code affect acces based CVE I	Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718			N/A		H-CIS-S 041119	
sg200-50fp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site				N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Scripting')			scriptiagain based vulne insuffice attack vulne persuinterfimalice subsets specification code affect acces based	ting (XSS st a user a linterfact rability ficient varied devices a linterfact rability rading a face to claim a linterfact rability fic web in A succes allow that arbitrate arbitrate in the content of	S) attack ce. The is due to alidation d input b terface of ce. An d exploit by user of t lick a access a nterface ssful exp ne attack rary scri ontext of face or ve brow ation.	veb- of the of the old				
sg200-50p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l	I interface Busines ged Swite an unaute act a crooting (XSS st a user linterface rability ficient vasupplied	ss-site S) attack of the v ce. The is due to alidation l input b terface o	and uld ated, web-	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			vulner persua interfa malici subsect specifi page. A could execut code i affecte access based	rability ading a ace to cl ous link quently ic web i A succes allow th te arbita n the co	user of to ick a and access a anterface ssful exponential exponent	che oloit cer to pt the				
sf300-08			12718	8						
31300-00			A vailn	erahilit	y in the	weh-				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Manag allow remot condu scripti agains based vulner insuffi user-s web-b affecte attack vulner persua interfa malici subsee	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface			N/A		H-CIS-S 041119	
CV Scoring Sca	lle 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			execu code affect acces based	allow the arbition the content of th	rary scri intext of face or ve brow ation.	pt the				
sf300-24										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability I interface Busines ged Swith an unaute attack act a crooking (XSS) st a user I interface rability ficient value cased interface ading a face to clain ading a face t	ce of Ciscs Smart teches conthenticater to ss-site S) attack to find the vector of the	and uld ated, web- on of y the of the this the che to pt the of the che to pt the of the che to pt t	N/A		H-CIS-S 041119	
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
sf300-24mp					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	N/A	H-CIS-SF30- 041119/1327
sf300-24p					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site	N/A	H-CIS-SF30- 041119/1328
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Scripting')			script again based vulne insuff user-web-laffect attack vulne persuinterf malic subset specific page. could execut code affect acces based	ting (XSS st a user a linterfact rability ficient varied devices and a linterfact for could be a linterfact for could be a linterfact for could be a linterfact for the could be a linterf	S) attack of the vece. The alidation of the terface of the exploit	veb- of of the of the oloit ser to pt the				
sf300-24pp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l	I interfa Busines ged Swi an unau te attack uct a cro ting (XSS st a user l interfa erability ficient va supplied	ss-site S) attack of the v ce. The is due to alidation l input b terface o	and uld ated, web-	N/A		H-CIS-S 041119	
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

sf300-48 A vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a				vulne persu interf malici subse specif page. could execu code i affect access based	rability ading a ace to cl ious link quently ic web i A succes allow th te arbita n the co ed inter s sensiti	by user of t ick a and access a nterface ssful exp ne attack rary scri ntext of face or ve brow ation.	he oloit er to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting') 16-10-2019 4.3 A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a	cf200 40			1271	8						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting') 4.3 Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a	31300 10					-					
page. A successful exploit	Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	4.3	Managallow remote conduscript agains based vulne insuff user-saffect attack vulne persuinterf malicisubse specifical	based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a						

(CVSS)

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
-6700 40			execu code affect acces based	allow the tearbite in the color ed inters sensiti information D: CVE-8	rary scri ontext of face or ve brow ation.	pt the				
sf300-48p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability l interface Busines ged Swir an unau te attack act a cro cing (XSS st a user l interface rability ficient va- supplied based in ed device act o cl ious link equently fic web i A succes allow the te arbitr in the co ed interface s sensiti l informat b: CVE- 8	ce of Ciscs Smart tches conthenticater to ss-site S) attack of the voce. The didation of the voce and exploit by user of the voce and access access and access access access access access and access a	and uld ated, web- on of y the of the this the coloit ser to pt the of t	N/A		H-CIS-S 041119	
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	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
sf300-48pp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	Mana allow remo conduscript again based vulne insuff user-web-laffect attack vulne persuinterf malic subset specific page. could execut code affect acces based CVE I	Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718					H-CIS-S 041119	
sf302-08										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site				N/A		H-CIS-S 041119	
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Scripting')			scriptiagain based vulne insuffice attack vulne persuinterfimalice subsets specification code affect acces based	ting (XSS st a user a linterfact rability ficient varied devices a linterfact rability rading a face to claim a linterfact rability fic web in A succes allow that arbitrate arbitrate in the content of	S) attack ce. The is due to alidation d input b terface of ce. An d exploit by user of t lick a access a nterface ssful exp ne attack rary scri ontext of face or ve brow ation.	veb- of of y the of the this che oloit ser to pt of the				
sf302-08mp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l	I interface Busines ged Swite an unaute act a crooting (XSS st a user linterface rability ficient vasupplied	ss-site S) attack of the v ce. The is due to alidation l input b terface o	and uld ated, web-	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			vulne persu interf malic subse specif page. could execu code i affect access based	rability ading a ace to cl ious link quently ic web i A succes allow th te arbita in the co	user of to ick a access a access a access a access a access a access are attacked access acce	che oloit cer to pt				
sf302-08mpp	2		1271	8						
\$1302-00mpj			A vulı	nerabilit	y in the	web-				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	Small Mana allow remote conduscript agains based vulne insuff user-s web-b affect attack vulne persu interf malic subse	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface		N/A		H-CIS-S 041119		
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			execu code affect acces based	allow the arbition the content of th	rary scri intext of face or ve brow ation.	pt the				
sf302-08p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability I interface Busines ged Swir an unaute attack act a crooking (XSS st a user interface rability icient value cased in ed device act could rability ading a face to cl ious link quently fic web i A succes allow the te arbite in the could seed interface seed interface allow the te arbite in the could the cou	ce of Ciscs Smart teches conthenticater to ss-site S) attack to find the vector of the	and uld ated, web- on of y the of the this the che to pt the of the che to pt the of the che to pt t	N/A		H-CIS-S 041119	
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
sf302-08pp					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	N/A	H-CIS-SF30- 041119/1337
sg300-10					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site	N/A	H-CIS-SG30- 041119/1338
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Scripting')			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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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- 12718							
sg300-10mp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An		N/A		H-CIS-S 041119			
CV Scoring Sca	le 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				Pato	h	NCIIP	CID
			attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-							
sg300-10mp	<u> </u>		1271	8						
	<u></u>		A vuli	nerabilit	y in the	web-				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	Small Mana allow remore conduscript again based vulne insuff user-s web-l affect attack vulne persu interf malic subse	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface					H-CIS-S 041119	
CV Scoring Sca	le 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	D	Description & CVE ID				h	NCIIP	CID
			execu code a affect acces based	could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID : CVE-2019-12718						
sg300-10p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability I interface Busines ged Swite an unaute attack act a cro cing (XSS st a user I interface based in the device action of the collection of the cate to clain on the cate to clain cate	ce of Ciscs Smart teches conthenticater to ss-site S) attack to find the vector of the	and uld ated, web- on of y the of the this the coloit ser to pt the of the of the coloit ser to pt of the o	N/A		H-CIS-S 041119	
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
sg300-10pp					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	N/A	H-CIS-SG30- 041119/1342
sg300-10sfp					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site	N/A	H-CIS-SG30- 041119/1343
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	D	escriptio	n & CVE I	D	Pato	ch	NCIIP	CID
Scripting')			scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718							
sg300-20										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An			N/A		H-CIS-S 041119		
CV Scoring Sca	le 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	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information.							
a~200 20				CVE ID : CVE-2019- 12718						
sg300-28			A vulr	nerabilit	y in the	web-				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit				N/A		H-CIS-S 041119	
CV Scoring Sca	ole 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	D	Description & CVE ID				h	NCIIP	CID
			execu code a affect acces based	could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID : CVE-2019-12718						
sg300-28mp			1271	8						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability an unaute attack act a crocing (XSS st a user linterfactorability ficient valued adding a face to claim a face to c	ce of Ciscs Smart teches conthenticater to ss-site S) attack to find the vector of the	and uld ated, web- on of y the of the this the chest to pt the of the chest to pt the ches	N/A		H-CIS-S 041119	
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
sg300-28p					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718	N/A	H-CIS-SG30- 041119/1347
amp_7150	<u>I</u>				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote	N/A	H-CIS-AMP 041119/1348
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	D	escriptio	n & CVE I	D	F	Patch	NCIIF	PCID
Scripting')			cross attacl web-l interf vulne insuff user- web-l interf could vulne persu interf link. A could execu code interf sensit inform	ker to co-site scrite scrite scrite scrite scrite scrite scrite sagainst based marginated as exploit rabilities ading a face to classed allow that arbitration the compation. D: CVE-8	ipting (X a user of anagements s are du alidation l input b anagement attacker these s by user of t ick a cra sful expl ne attack cary scri ontext of ccess wser-ba	e to of y the ent che afted loit ser to pt				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these				N/A		H-CIS-A 041119	
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
			vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15269		
amp_8150					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based	N/A	H-CIS-AMP 041119/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. CVE ID : CVE-2019- 15268		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269	N/A	H-CIS-AMP 041119/1351
aironet_1540)				
Improper Privilege Managemen t	16-10-2019	10	A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated, remote attacker to gain unauthorized access to a	N/A	H-CIS-AIRO- 041119/1352
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6 840	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pato	ch	NCIIF	CID
			elevativulne insuff for ce affect attack vulne requestion attack privil attack grant possil option attack informsome of the including the deprivil attack informsome of the including th	ted device ted privice rability in the could a certo gas evice with eges. Where would ed acces ble confing wire choose ding wire condition at the condition of the confing wire choose ding wire condition at the condition of the	leges. The second and the second are second and the second allow the second allow ew sension are play with valuing, seless able the sable the sabl	this this KLs an e s to e tive tive ace lues n. It AP, arvice ients				
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	Contr of Wi (CAPV imple Airon Acces allow adjace	nerability of and Pareless Act WAP) presentation et and Case Points an unaugent attact ected de	rovision ccess Po otocol on of Cis atalyst 9 (APs) co thentica	ints sco 9100 ould ated,	N/A		H-CIS-A 041119	
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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			result service The vimpromana CAPW proces could vulne high vireles frame to an succe allow a devial a DoS assoc CVE I	ct unexporting in a secondition of the attack of the attac	denial o condition ility is durce during sage attacked this by sending a short device. A cloit councier to contact the contact in the Allian in for clith the Allian in for cl	er ng a nate time A ld cause				
Improper Input Validation	16-10-2019	2.1	A vulibridg (BPD) functi Airon (APs) unaut attacl port t disabl vulne becaut from client incorr could vulne wirele	A vulnerability in the bridge protocol data unit (BPDU) forwarding functionality of Cisco Aironet Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an AP port to go into an error disabled state. The vulnerability occurs because BPDUs received from specific wireless clients are forwarded incorrectly. An attacker could exploit this vulnerability on the wireless network by sending a steady stream of		N/A		H-CIS-A 041119		
CV Scoring Scal	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Des	Description & CVE ID				h	NCIIP	C ID
aironat 1560			success allow t a limite (DoS) a	sful exphe attaed deniattack between the could of the could or the cou	frames. cloit cou cker to c al of ser because go offlin	ld cause vice an				
aironet_1560										
Improper Privilege Managemen t	16-10-2019	10	Airone (APs) Sallow a remote unauth targete elevate vulnera insufficion certaffecte attacke vulnera reques from attacke privile attacke grante possible options attacke inform some of their includi	t Accessoftwar an unaute attack acrized device device ability ting spendice with a could accessive would accessive to vice with a ccessive to vice ation a could accessive to vice ation accessive to vice accessive to	leges. This due to coess con and exploit the dependent of the devatable the development of the development o	ated, in o a ne ntrol a this e s to e tive tive lice lues	N/A		H-CIS-A 041119	
CV Scoring Sca	le 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	Descri	ption & CVE I	D	Pato	:h	NCIIPC ID		
			attacker to creating a (DoS) con associated							
			15260	VL 2017						
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	of Wireless (CAPWAP) implement Aironet ar Access Polallow and adjacent a an affected restart under resulting is service (Dar The vulned improper managem CAPWAP) processing could exployulnerability high volumerability wireless in frames with to an affect successful allow the adevice to unexpected a DoS con associated.	ent during message g. An attacke loit this lity by sending of legiting anagement thin a short eted device. I exploit countattacker to design the device attacker to design the device attacker to design the device attacker to design the design that a short countage is attacker to design the design that a short countage is attacker to design the design that a short countage is a short countage is a short a short countage is a short a short countage is a short a	ints sco 9100 ould ated, ause f on. ue to er ang a nate time A ld cause ag in ients	N/A		H-CIS-A 041119		
Improper Input	16-10-2019	2.1		bility in the otocol data ı	ınit	N/A		H-CIS-A 041119		
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-		5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	De	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Validation			(BPDU function Aironal (APs) unaut attack port to disable vulner because from some could vulner wirelessendir crafted allow a limit (DoS) AP port	J) forward on ality of the theorem o	arding of Cisco as Points allow an ted, adja use an A o an erro a. The occurs Us receiv wireless warded n attack this on the vork by ady strea frames. oloit cou cker to o al of ser pecause	cent IP or ved er A Id cause vice an				
aironet_1800)									
Improper Privilege Managemen t	16-10-2019	10	A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated, remote attacker to gain unauthorized access to a targeted device with elevated privileges. The vulnerability is due to insufficient access control for certain URLs on an affected device. An attacker could exploit this vulnerability by				N/A		H-CIS-A 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			from explo attack the deprivil attack possil option attack informsome of the include network would attack creati (DoS) associ	esting spean affect it could a ser to gate evice with ed accessole configure to vice mation at options of conditions and also all ser to distance with ed accessole configure evice configure evice ev	ted AP. A allow the in access the elevate of all guration allow sension of replaying, eless iguration ow the sable the on for cloth the Allow the allow the allow the sable the on for cloth the Allow the all	an e s to ed the tive ace lues n. It e AP, rvice ients				
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol implementation of Cisco Aironet and Catalyst 9100 Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management during CAPWAP message processing. An attacker			N/A		H-CIS-A 041119		
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
			could exploit this vulnerability by sending a high volume of legitimate wireless management frames within a short time to an affected device. A successful exploit could allow the attacker to cause a device to restart unexpectedly, resulting in a DoS condition for clients associated with the AP. CVE ID: CVE-2019- 15264		
Improper Input Validation	16-10-2019	2.1	A vulnerability in the bridge protocol data unit (BPDU) forwarding functionality of Cisco Aironet Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an AP port to go into an error disabled state. The vulnerability occurs because BPDUs received from specific wireless clients are forwarded incorrectly. An attacker could exploit this vulnerability on the wireless network by sending a steady stream of crafted BPDU frames. A successful exploit could allow the attacker to cause a limited denial of service (DoS) attack because an AP port could go offline. CVE ID: CVE-2019-	N/A	H-CIS-AIRO- 041119/1360

Weakness	Publish Date	cvss	Description & CVE ID	Patc	h	NCIIPC ID	
			15265				
aironet_2800)						
Improper Privilege Managemen t	16-10-2019	10	A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated, remote attacker to gain unauthorized access to a targeted device with elevated privileges. The vulnerability is due to insufficient access control for certain URLs on an affected device. An attacker could exploit this vulnerability by requesting specific URLs from an affected AP. An exploit could allow the attacker to gain access to the device with elevated privileges. While the attacker would not be granted access to all possible configuration options, it could allow the attacker to view sensitive information and replace some options with values of their choosing, including wireless network configuration. It would also allow the attacker to disable the AP, creating a denial of service (DoS) condition for clients associated with the AP. CVE ID: CVE-2019- 15260	N/A		H-CIS-A 041119	
Uncontrolle	16-10-2019	6.1	A vulnerability in the	N/A		H-CIS-A	IRO-
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 848	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
d Resource Consumptio n	Publish Date	CVSS	Controf Wi (CAP) imple Airon Access allow adjaces an aff restal service The vimpro mana CAPW proces could vulne high virel frame to an succes	reless Active and Control of the Active and Control of the Active and Control of the Active and the Active	rovision ccess Pootocol on of Cistallyst 9 (APs) continued the condition of Cistallyst 9 (APs)	aing ints sco 9100 ould ated, ause fon. ue to er ing a nate time A ld	Pato	ch	NCIIF 041119	
			a dev unexț a DoS assoc	ice to respectedly, condition in the attack with the attack wi	start , resultir on for cli th the Al	ng in ients				
Improper Input Validation	16-10-2019	2.1	bridg (BPD) funct Airon (APs) unaut attach port t	nerabilite protocutionality of the Accest could alst the carto carto go into led state	ol data un ding of Cisco es Points llow an ted, adjause an A	cent .P	N/A		H-CIS-A 041119	
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	Pato	h	NCIIP	C ID
			vulnerability occurs because BPDUs received from specific wireless clients are forwarded incorrectly. An attacker could exploit this vulnerability on the wireless network by sending a steady stream of crafted BPDU frames. A successful exploit could allow the attacker to cause a limited denial of service (DoS) attack because an AP port could go offline. CVE ID: CVE-2019- 15265				
aironet_3800)						
Improper Privilege Managemen t	16-10-2019	10	A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated, remote attacker to gain unauthorized access to a targeted device with elevated privileges. The vulnerability is due to insufficient access control for certain URLs on an affected device. An attacker could exploit this vulnerability by requesting specific URLs from an affected AP. An exploit could allow the attacker to gain access to the device with elevated privileges. While the attacker would not be granted access to all	N/A		H-CIS-A 041119	
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	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			option attack inform some of the include network would attack creati (DoS) associ	ble configues, it counter to view nation and options of configues and also allower to distend the condition of the condition	ld allowed sew sension and replaced with valuing, beless ow the sable the sable the confor click the Allower sension for click the Allower sension sen	the tive ace lues n. It e AP, rvice ients				
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol implementation of Cisco Aironet and Catalyst 9100 Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management during CAPWAP message processing. An attacker could exploit this vulnerability by sending a high volume of legitimate wireless management frames within a short time to an affected device. A successful exploit could				N/A		H-CIS-A 041119	
			anow	the attac	cker to d	cause				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a device to restart unexpectedly, resulting in a DoS condition for clients associated with the AP.		
			CVE ID : CVE-2019- 15264		
Improper Input Validation	16-10-2019	2.1	A vulnerability in the bridge protocol data unit (BPDU) forwarding functionality of Cisco Aironet Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an AP port to go into an error disabled state. The vulnerability occurs because BPDUs received from specific wireless clients are forwarded incorrectly. An attacker could exploit this vulnerability on the wireless network by sending a steady stream or crafted BPDU frames. A successful exploit could allow the attacker to cause a limited denial of service (DoS) attack because an AP port could go offline. CVE ID: CVE-2019-15265	N/A	H-CIS-AIRO- 041119/1366
aironet_4800)				
Improper Privilege Managemen t	16-10-2019	10	A vulnerability in Cisco Aironet Access Points (APs) Software could allow an unauthenticated remote attacker to gain unauthorized access to a	N/A	H-CIS-AIRO- 041119/1367
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5- 852	6 6-7	7-8 8-9 9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	ch	NCIIF	CID
			elevativulne insuff for ce affect attack vulne requestion attack privil attack grant possil option attack informsome of the including the deprivil attack informsome of the including th	ted device ted privice rability in the could a certo gas evice with eges. Where would ed acces ble confing, it could a certo vice mation a coptions of choose ding wire choose ding wire choose ding a den condition a conditi	leges. The second control of the con	this this KLs an e s to e tive tive ace lues n. It AP, arvice ients				
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	Contr of Wi (CAPV imple Airon Acces allow adjace	nerability ol and Pareless Act WAP) presentation et and Case Points an unautent attact ected de	rovision ccess Po otocol on of Cis atalyst 9 (APs) co thentica	ints sco 9100 ould ated,	N/A		H-CIS-A 041119	
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
			restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management during CAPWAP message processing. An attacker could exploit this vulnerability by sending a high volume of legitimate wireless management frames within a short time to an affected device. A successful exploit could allow the attacker to cause a device to restart unexpectedly, resulting in a DoS condition for clients associated with the AP. CVE ID: CVE-2019-		
aironat 1910)		15264		
Improper Input Validation	16-10-2019	7.8	A vulnerability in the Point-to-Point Tunneling Protocol (PPTP) VPN packet processing functionality in Cisco Aironet Access Points (APs) could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Generic Routing Encapsulation (GRE) frames that pass through	N/A	H-CIS-AIRO- 041119/1369

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the data plane of an affected AP. An attacker could exploit this vulnerability by associating to a vulnerable AP, initiating a PPTP VPN connection to an arbitrary PPTP VPN server, and sending a malicious GRE frame through the data plane of the AP. A successful exploit could allow the attacker to cause an internal process of the targeted AP to crash, which in turn would cause the AP to reload. The AP reload would cause a DoS condition for clients that are associated with the AP.		
aironet_1830			15261		
Improper Input Validation	16-10-2019	7.8	A vulnerability in the Point-to-Point Tunneling Protocol (PPTP) VPN packet processing functionality in Cisco Aironet Access Points (APs) could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Generic Routing Encapsulation (GRE) frames that pass through	N/A	H-CIS-AIRO- 041119/1370

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the data plane of an affected AP. An attacker could exploit this vulnerability by associating to a vulnerable AP, initiating a PPTP VPN connection to an arbitrary PPTP VPN server, and sending a malicious GRE frame through the data plane of the AP. A successful exploit could allow the attacker to cause an internal process of the targeted AP to crash, which in turn would cause the AP to reload. The AP reload would cause a DoS condition for clients that are associated with the AP.		
			CVE ID : CVE-2019- 15261		
aironet_1850)		A vulnerability in the		
Improper Input Validation	16-10-2019	7.8	Point-to-Point Tunneling Protocol (PPTP) VPN packet processing functionality in Cisco Aironet Access Points (APs) could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Generic Routing Encapsulation (GRE) frames that pass through	N/A	H-CIS-AIRO- 041119/1371

4-5

5-6

3-4

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
			affect could vulne assoc AP, in conne PPTP sendi frame plane succe allow an int targe which the A reload condi are as	exploiterability iating to atting to very serion to VPN sering a male through of the Adversal predefer and turn P to relod would attion for ssociated to: CVE	this by a vulne a PPTP ver, and licious Gh the data. P. A coloit counces of crash, would counce a clients the district the cause a clients the district the counce a clients the district the cause a clients the cause a client the cause	rable VPN trary I RE ta Ild cause The Cause AP DoS hat				
5508_wireles	ss_controllers									
Improper Input Validation	16-10-2019	7.8	Secur mana Wirel (WLC allow remo denia condi devic exists proce delete conne disco could	gement less LAN (a) Softwar an unau te attack (b) of service. The vice because ess is not ed when ection to	for Cisco Control are could thentica are to ca ice (DoS an affect ulnerabi e the SSI proper an SSH the dev An atta	ller d ated, use a d lity H ly	N/A		H-CIS-5 041119	
CV Scoring Sca	le 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
			repeatedly opening SSH connections to an affected device. A successful exploit could allow the attacker to exhaust system resources by initiating multiple SSH connections to the device that are not effectively terminated, which could result in a DoS condition. CVE ID: CVE-2019-15262		
5520_wirele	ss_controllers				
Improper Input Validation	16-10-2019	7.8	A vulnerability in the Secure Shell (SSH) session management for Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the SSH process is not properly deleted when an SSH connection to the device is disconnected. An attacker could exploit this vulnerability by repeatedly opening SSH connections to an affected device. A successful exploit could allow the attacker to exhaust system resources by initiating multiple SSH connections to the device that are not effectively terminated,	N/A	H-CIS-5520- 041119/1373

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
catalyst_9100)		which could result in a DoS condition. CVE ID: CVE-2019- 15262		
Uncontrolle d Resource Consumptio n	16-10-2019	6.1	A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol implementation of Cisco Aironet and Catalyst 9100 Access Points (APs) could allow an unauthenticated, adjacent attacker to cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to improper resource management during CAPWAP message processing. An attacker could exploit this vulnerability by sending a high volume of legitimate wireless management frames within a short time to an affected device. A successful exploit could allow the attacker to cause a device to restart unexpectedly, resulting in a DoS condition for clients associated with the AP. CVE ID: CVE-2019-15264	N/A	H-CIS-CATA- 041119/1374
firepower_m	anagement_ce		600		
Improper	16-10-2019	3.5	Multiple vulnerabilities in	N/A	H-CIS-FIRE-
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6 859	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')			mana Cisco Mana (FMC authe attack cross attack web-k interf vulne insuff user-s web-k interf could vulne persu interf link. A could execu code i	reb-based gement of could a enticated are to consider a considerated are to consider a considerated are to considerated and are to considerated are to considerated are to considerated are to considerate arbitrate arb	interface ver Center Illow an , remote nduct a pting (X a user of anagement input by anagement attacker these is by user of t ick a cra isful expl are attack ary scrip ntext of ccess wser-base	esss) of the ent e to of y the ent he fted oit er to pt the			041119	/1375
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross attack web-l	ple vulne feb-based gement (Firepow gement () could a enticated ker to cor site scri k against based ma	d interface rer Center Ilow an , remote nduct a pting (X a user c	e of ess) of the	N/A		H-CIS-F 041119	
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	D	escription	n & CVE I	D	Pato	ch	NCIIP	CID
			insuff user-s web-l interf could vulne persu interf link. A could execu code interf sensit inform	rabilities rabilities supplied based ma face. An a exploit the rabilities ading a uface to climate arbitrin the conface or active, brownation.	alidation input be anagementtacker these is by user of t ick a cra sful expl are attack ary scri intext of ccess wser-ba	the of oit cer to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interf Firep Center an un remore condustript again based interf vulne insuff user-sweb-linterf could vulne persuinterf link.	nerability I manage face of Ci ower Maer (FMC) authentite attack act a crossing (XSS st a user I manage face. The rability is ficient valued based maexploit to a capility I rability I rab	ement sco inageme could al cated, er to ss-site d) attack of the v ement is due to ilidation input b anageme attacker this by user of t ick a cra sful expl	ent llow veb- o of y the ent che	N/A		H-CIS-F 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
			execute arbitrary script code in the context of the interface or access sensitive, browser-based information. CVE ID: CVE-2019- 15270							
firepower_ap	opliance_7030									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulner insuff user-web-linterf could vulner persuinterf link. A could execut code interf sensitinform	ple vulnoreb-based gement (for the constitution of the constitutio	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement input be anagement input be are attacker intext of ceess wiser-based	e of (SS) of the ent e to of y the ent the afted oit cer to pt the	N/A		H-CIS-F 041119	
Improper Neutralizati	16-10-2019	3.5		Multiple vulnerabilities in the web-based					H-CIS-F	IRE-
CV Scoring Sca (CVSS)	o-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
on of Input During Web Page Generation ('Cross-site Scripting')			manag Cisco I Manag (FMC) auther attack cross-s attack web-b interfa vulner insuffi user-s web-b interfa could of vulner persua interfa link. A could a execut code in inform	gement Firepow gement could a nticated er to co site scri against ased m ace. The cient va upplied ased m ace. An a exploit rabilitie ading a ace to cl succes allow th te arbit n the co ace or a ive, bro nation. C: CVE	interface ver Center allow an l, remote nduct a ipting (X c a user of anagement is se s are du- alidation l input b anagement attacker these s by user of t ick a cra sful explance attack cary scri- ontext of ccess wser-ba	e of e SS) of the ent e to of y the ent the afted oit aer to pt the			041119	
firepower_ap	ppliance_7110									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management				N/A		H-CIS-F 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			insuff user-s web-l interf could vulne persu interf link. A could execu code s interf sensit inform	vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-						
			1526	8						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-sweb-linterf could vulne persuinterf	ple vulne eb-based gement if Firepow gement if Could a inticated cer to con- site script cased mate cace. The rabilities cace. An a exploit if rabilities ading a if ace to clipt cace to clipt cace success	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement input by anagement attacker these s by user of t	es of established	N/A		H-CIS-F 041119	
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
firepower a	opliance_7115		could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. CVE ID: CVE-2019-15269		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268	N/A	H-CIS-FIRE- 041119/1382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269	N/A	H-CIS-FIRE- 041119/1383
firepower_m	anagement_ce	nter_v	irtual_appliance		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS)	N/A	H-CIS-FIRE- 041119/1384
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			interficulting vulne insufficulting vulne persuinterficulting could execute code interfisensity information. CVE I	web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15268 Multiple vulnerabilities in						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-sweb-linterf could vulne	ple vulne eb-based gement (Firepow gement () could a enticated ker to co -site scri k against cased ma face. The rabilities supplied based ma exploit (rabilities ading a	d interface ver Center cllow an , remote nduct a pting (X a user of anageme se s are due input b anageme attacker these s by	e of SSS) of the ent e to of of y the ent	N/A		H-CIS-F 041119	
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	De	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			link. A could executode interface sensitinform	asucces allow the arbiton the coace or a live, bro nation. D: CVE-9	wser-ba - 2019-	oit er to pt the sed				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interfacent interfacent insuff user-s web-based interfacent information interfacent	manage ace of Cower Mar (FMC) authent the attack act a croing (XSS at a user manage ace. The rability ace to classed mace ace to classed the arbitranthe coace or a live, broination. D: CVE-	isco anageme could al icated, ser to ss-site c) attack of the v ement is due to alidation l input b anageme attacker this by user of t ick a cra sful expl ne attack cary scri ontext of ccess wser-ba	ent clow veb- cof y the ent he afted oit aer to pt the	N/A		H-CIS-F 041119	
CV Scoring Sca	le 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
firepower_ap	ppliance_7125		L		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268	N/A	H-CIS-FIRE- 041119/1387
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS)	N/A	H-CIS-FIRE- 041119/1388

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these	N/A	H-CIS-FIRE- 041119/1389

2-3

0-1

CV Scoring Scale

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15268		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information.	N/A	H-CIS-FIRE- 041119/1390

Weakness	Publish Da	te CVSS	D	escriptio	n & CVE I	D		Pato	:h	NCIIF	C ID
			CVE I 1526	D : CVE- 9	2019-						
firepower_ap	pliance_71	120									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-201	3.5	the wimana Cisco Mana (FMC) author attack cross attack web-linterf vulner insuff user-web-linterf could vulner persuinterf link. A could execute code interf sensitinform	ple vulnateb-based gement (Firepowers) could a	interface ver Center allow an l, remote nduct a ipting (X c a user of anagement is s are dural alidation l input b anagement attacker these s by user of t ick a crassful explance attacker ary scription text of ccess wser-ba	e of (SS) of the ent e to of y the ent che afted oit cer to pt the	N/	'A		H-CIS-F 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-201	3.5	the w mana Cisco Mana (FMC	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote				'A		H-CIS-F 041119	
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	Descript	ion & CVE I	D	Pato	h	NCIIP	C ID
Scripting')			attacker to de cross-site so attack again web-based interface. The vulnerability insufficient user-supplied web-based interface. And could explosively vulnerability persuading interface to link. A successful allow execute arbused in the face or sensitive, businformation CVE ID: CV 15269	conduct a cripting (X st a user of managements are duvalidation ed input be managements by a user of telick a craessful explication extending the attack itrary scriptontext of access cowser-band.	ass) of the ent e to of of y the ent the afted oit aer to pt				
firepower_ap	ppliance_7010								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulte web-base managemer Cisco Firepo Managemer (FMC) could authenticate attacker to coross-site so attack again web-based interface. The vulnerability insufficient user-supplied web-based in the counter face.	sed at interface ower at Center al allow an ed, remote conduct a cripting (X est a user of managements ies are du validation ed input b	e of (SS) of the ent e to a of y the	N/A		H-CIS-F 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
				vulne persu interf link. A could execu code i interf sensit inform	uld exploit these Inerabilities by rsuading a user of the terface to click a crafted ak. A successful exploit uld allow the attacker to ecute arbitrary script de in the context of the terface or access asitive, browser-based formation. TE ID: CVE-2019- 6268 ultiple vulnerabilities in e web-based						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-20	019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-sweb-linterf could vulne persuinterf link. A could execute code interf	gement Firepow gement Could a Inticated Ker to co Site scrip K against Dased m Cace. The Ficient va Supplied Dased m Cace. An a exploit rabilitie Lading a face to cl A succes allow th Lite arbita in the co	interfactiver Center Allow an I, remote anduct a ipting (X a user of an agement attacker these is by user of the attacker ary scripontext of	e of (SS) of the ent e to of y the ent che afted oit cer to pt the	N/A		H-CIS-F 041119	
CV Scoring Sca (CVSS)	le 0 -1	1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIF	PC ID
			infori	nation.						
			CVE I 1526	D : CVE- 9	2019-					
firepower_ap	pliance_8370									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-sweb-linterf could vulne persuinterf link. A could execut code interf sensitinform CVE I 1526		dinterface ver Center allow an , remote nduct a pting (X a user of anageme attacker these s by user of t ick a cra sful expl ne attack cary scri ntext of ccess wser-ba	e of SSS) of the ent e to of ythe ent the oft the sed	N/A		H-CIS-F 041119	
Improper Neutralizati on of Input During Web Page	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center				N/A		H-CIS-F 041119	
Generation			(FMC) could allow an							
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	De	escriptio	n & CVE I	D	Pate	h	NCIIP	CID
('Cross-site Scripting')			authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15269							
firepower_m	anagement_ce	nter_1	600							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the		N/A		H-CIS-F 041119			
CV Scoring Sca	le 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	D	escription	n & CVE I	D	Pat	ch	NCIIP	C ID
			interf could vulne persu interf link. A could execu code i interf sensit inform	pased marace. An a exploit from the contact of the	attacker these s by user of t ick a cra sful expl ne attack rary scri ntext of ccess wser-ba	the oit er to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attackers attackers web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuing code in the could execuing the could execuing the could execuing the code in the could execuing the code in the could execuing the code in the code i	ple vulne eb-based gement if Firepow gement of the control of the	d interface ver Center illow an , remote nduct a pting (X a user of anageme is are du ilidation input b anageme these s by user of t ick a cra sful expl ne attack rary scri ntext of	e of (SS) of the ent e to of y the ent che afted oit cer to pt	N/A		H-CIS-F 041119	
CV Scoring Sca	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	D	escriptior	n & CVE II	D	Pato	h	NCIIP	CID
Weakness	Publish Date	CVSS	sensiti inform CVE I 1526 A vuln based interf Firepo Center an un remore conduscript again.	tive, brown nation. D : CVE-	y in the ement sco anagement cated, er to ss-site of the w	web-	Patc	h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	interf vulne insuff user-s web-l interf could vulne persu interf link. A could execu code i interf sensit inform	race. The rability is cient valued as a ce. An a exploit the rability because allow the arbitration the contact of a ce. The contact of	is due to ilidation input be anagement attacker this by user of t ick a cra sful expl ice attack ary scri ntext of ccess wser-ba	he of ter to pt the	N/A		H-CIS-F 041119	
firepower_ap	pliance_7020		1327							
Improper			Multi	ple vulne	erabiliti	es in				
Neutralizati on of Input During Web Page	16-10-2019	3.5	mana Cisco	eb-based gement i Firepow gement (interfac ver	e of	N/A		H-CIS-F 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
Generation ('Cross-site Scripting')			auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execut code interf sensitinform CVE I	_	, remote nduct a pting (X a user of anagement se s are ductal alidation input be anagement attacker these s by user of to ick a crassful explance attacker ary scriintext of access wser-ba	esss) of the ent e to of of y the ent the oft the ter to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attack cross attack web-l interf vulne insuff user-s	CVE ID: CVE-2019- 15268 Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management					H-CIS-F 041119	
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	·		Patch	NCIIPC ID
			interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269		
firepower_ap	ppliance_8130				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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	N/A	H-CIS-FIRE- 041119/1402

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			sensit inforr	ace or active, brown ation. D: CVE-	wser-ba	sed				
			1526	8						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attack cross-attack web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuinterf sensit inform	ple vulne eb-based gement in the colar to character to contain the colar to character to charact	dinterface fer Center llow an , remote nduct a pting (X a user of anagement input be anagement input be are attacker are attacker are attacker intext of excess wser-ba	e of SSS) of the ent e to of y the ent he afted oit aer to pt the	N/A		H-CIS-F 041119	
sg550x-24										
Cross-Site Request Forgery	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and				N/A		H-CIS-S 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	PC ID
(CSRF)			allow remo condured to the tauser he privil could configured to the conduction of the tauser he privil could configured to the tauser he	D : CVE-	ithenticater to ss-site ry (CSRF ffected ulnerabilitient Corthe we ement on affected acker coulnerability a user of following a user of following a user of following a country actillege levelser. If the inistrative attacker is eattacker attacker of cause a fice (DoS an affected for affected	ated, ility CSRF eb- ed ould lity of a ld ions el of ne er e				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again	nerabilit l interface Busines ged Switt an unau te attack act a crost ing (XSS st a user l interface	ce of Ciso es Smart tches con thentica er to ess-site of the w	and uld ated,	N/A		H-CIS-S 041119	
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	Descr	ription	& CVE II	D	Pato	h	NCIIP	CID
			vulnerabinsufficie user-sup web-base affected e attacker vulnerab persuadi interface malicious subseque specific v page. A s could alle execute a code in the affected in access see based info	ent valided interest of the contract of the co	idation input by erface of . An exploit y ser of to ek a and ccess a terface ful exp e attack ry scri text of ce or e brow ion.	of y the of the this he oloit ter to pt the				
sg550x-24m	D		12710							
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based mainterface Business Managed allow an remote a conduct a request f attack on system. T is due to protection based mainterface device. A	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability					H-CIS-S 041119	
CV Scoring Sca	le 0-1	1-2	2-3 3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pato	h	NCIIP	CID
			malic succe allow perfor with t the ta user h privil could config comm denia condi	D : CVE-	A cker to rary active ser. If the nistrative execute cause a ce (DoS an affect	ld ions el of ne ve or				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remote condu script agains based vulne insuff user-s web-b affect attack vulne persu interf malic subse specif page.	nerability l interface Busines ged Switt an unau te attack act a cross cing (XSS st a user l interface rability if ficient va supplied based inte ed device act could rability l ading a u face to cli ious link equently fic web in A success allow th	te of Ciso s Smart ches con thentica er to ss-site) attack of the w ee. The s due to lidation input by terface of ee. An l exploit by user of t ick a and access a nterface	and ald ated, veb- of the this he	N/A		H-CIS-S 041119	

Weakness			Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718		
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected	N/A	H-CIS-SG55- 041119/1408

Weakness	Publish Date	CVSS	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
			device CVE I 1263	D : CVE-	2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remore conduscript again based vulne insuff user-s web-l affect attack vulne persu interf malic subse specif page. could execu code i affect acces based	nerability l interface Busines ged Switt an unaute attack act a cross st a user l interface rability if ficient value supplied based interface ading a user lading a user	the of Cisos Smart sches conthenticater to ss-site of the ware. The sidue to didation input by the exploit of the art and access access and access access access and access and access and access access access access and access	and uld ated, web- of the this the coloit ter to pt the	N/A		H-CIS-S 041119	
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interf Busin	nerability I manage Tace of Ci ess Smar	ement sco Sma rt and	ıll	N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	Managed Switches could 2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			allow remore condustreques attack system is due prote based interfedevice explosion by performation with the tauser hyprivilic configuration denial condition of the condition o	an unaute attack act a cross st forger on an am. The vertions for a constant actions for a constant actions at this vertice attact the attact actions link as admitted actions admitted actions and action on a constant action action action on a constant action on a constant action ac	ithenticater to ss-site ry (CSRF ffected ulnerability of the weeken to acker to rary act lege level instrative attacker to rary act lege finistrative attacker to rary act an affect are to a serious an affect and affect and affect and affect and affect and affect are to a serious an affect and affect and affect and affect and affect and affect are to a serious and affect and affect and affect are to a serious and affect and affect and affect are to a serious and affect and affect are to a serious and affect are to a serious and affect and affect are to a serious and a seriou	ated, F) ility CSRF eb- ed ould lity of r a lld ions el of ne eve er e				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based	nerabilit l interface Busines ged Swit an unau te attack act a crost ing (XSS st a user l interface rability i	ce of Ciso es Smart tches con athentica er to ess-site of attack of the w	and uld ated,	N/A		H-CIS-S 041119	
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	Descriptio	n & CVE II)	Pato	h	NCIIP	C ID
			insufficient v user-supplied web-based in affected device attacker coul vulnerability persuading a interface to c malicious lin subsequently specific web page. A succe could allow t execute arbit code in the co affected inter access sensit based inform CVE ID: CVE 12718	d input by terface of ce. An d exploit by user of the lick a k and access a interface essful explorate of face or ive brows action.	this loit er to pt the				
sg550x-48									
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerabili based managinterface of Computer attack on an asystem. The vision device. An attexploit this viby persuadinterface on a the interface on a the interfac	tement disco Sma art and art and atches counthentical der to a constant of the western of the western affected art affecte	ll ald ated, lity SRF b- ad ald aty of	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	a & CVE II	D	Pato	:h	NCIIP	C ID
			succe allow perfor with t the ta user h privil- could config comm denia condi- device	D : CVE-	cker to cker to rary active ser. If the nistrative attacked executed cause a ce (DoS	ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remote condu script agains based vulne insuff user-s web-baffect attack vulne persu interf malic subse	nerability l interface Busines ged Switt an unau te attack act a cross cing (XSS st a user l interface rability if ficient va supplied based inte ed device cer could rability be lading a u face to cli ious link equently fic web in	te of Ciso s Smart ches con thentica er to ss-site) attack of the w ee. The s due to lidation input by terface of ee. An l exploit by user of t ick a and access a nterface	and uld ated, veb-	N/A		H-CIS-S 041119	
				allow th	e attack	er to				

Weakness	Publish Date	cvss	De	scription	a & CVE II	D	Pato	h	NCIIP	CID
			affecte access based	d interf	ve brow ntion.					
			12718							
sg550x-48m	p									
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interfa Busines Manag allow a remote conductive exploits by perturbed based interfated devices allow the interfated based interfated by perturbed by perturbed by perturbed by perform with the tartuser has priviled could a configuration of the could be	manage ace of Circess Smar ged Switten unau e attack act a cross on an act at this vurations for manage ace on an act this vurations for arbiting privile act	sco Smart and sches continued thentical er to ss-site ffected ulnerability of the weeken to affecte acker coulnerability a user of following a continued to following a con	uld ated, ility CSRF eb- ed ould lity of a ld ions el of ne ve er	N/A		H-CIS-S 041119	
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 Dat	te CVSS	D	escriptio	n & CVE II	D	Pat	ch	NCIIP	C ID
			CVE I 1263	D : CVE- 6	2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-201	9 4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerabilitical interface Business ged Swift an unaute attack act a crooking (XSS is a userability facient value ading a face to claim ading a face arbitration and a face arbitration arbitration and a f	ce of Ciscos Smart teches continued to ss-site of the vector of the vector of the continued to stand access a context of face or ve brown ation.	and uld ated, web- of the this the coloit ser to pt the the	N/A		H-CIS-S 041119	
sg550x-48p										
Cross-Site Request Forgery (CSRF)	16-10-201	9 6.8	based interf Busin Mana	nerabilit I manage Tace of Ci ess Sma ged Swit an unau	ement sco Sma rt and tches co	all uld	N/A		H-CIS-S 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			condureque attack system is due prote based interfedevice explo by pethe immalic succe allow perforwith the tauser keyprivil could configure comments of the could configure conditions of the could configure conditions of the could configure conditions of the could conditions of the could configure conditions of the could condition of the condition of	D : CVE-	ss-site ry (CSRF ffected ulnerabi fficient Cor the we ement n affecte acker co ulnerabil g a user o co follow a. A bloit cou cker to rary act lege leve ser. If th nistrativ e attacke c cause a ice (DoS an affect	ed uld iity of a ld ions el of ne ve				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remore condu script again based vulne	nerability I interface Busines ged Swite an unau te attack act a crost ing (XSS st a user I interface rability i	ce of Ciso s Smart ches con thentica er to ss-site of the w ce. The	and ald ated, veb-	N/A		H-CIS-S 041119	
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	De	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			web-baffector attack vulner persurinterfamalici subsers pecifipage. Could execured access based	pased in ed device rability ading a ace to clious link quently ic web i A succestallow the arbitron the coed interpolation and th	d exploit by user of t ick a access a nterface ssful exp ne attack cary scri ontext of face or ve brow ation.	this the color of				
2250-246			1271	8						
sg550xg-24f			A vulr	nerabilit	y in the	web-				
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interfar Busing Allow remote conducting attack system is due protection based interfar devices exploit by per the interfar and the interfar attack system is due to base at a conduction by per the interfar attack system is due to base at a conduction by per the interfar attack system in the interfar attack system.	manage ace of Circles Smarged Swirt an unaute attack act a crost forge acon an amount of the circles on an ace on ace. An attack act a this vursuading	ement isco Sma rt and tches co athentica ter to ss-site ry (CSRI affected ulnerab fficient (or the we ement n affecte acker co alnerabi g a user to follow	uld ated, ility CSRF eb- ed ould lity	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
			allow performithe tarend to the tarend to th	D : CVE-	cker to rary acti lege leve ser. If th nistrativ attacke e e execute cause a ice (DoS	ions el of ne ve er				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remote conduscript agains based vulne insuff user-s web-b affect attack vulne persu interf malici subse specif page. could execu	nerability l interface Business ged Switt an unau te attack act a cross cing (XSS st a user l interface rability i ficient va supplied based inte ed device cer could rability be ading a u face to cli ious link equently a fic web in A success allow th te arbitr	the of Ciscons Smart sches constituted in the ntical ser to see site of the way and input by the face of the cary soriginal exploit and access access access and access access access access and access acces	and uld ated, web- of the of the chis che of the chis che of the chis che of the chis che	N/A		H-CIS-S 041119	
			code i	in the co	ntext of	the	l			

Weakness	Publish Date	cvss	Description & CVE ID	Pato	:h	NCIIP	CID
			affected interface or access sensitive browserbased information.				
			CVE ID : CVE-2019- 12718				
sg550xg-24t			12/10				
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-	N/A		H-CIS-S0 041119,	
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	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
			1263	6						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability I interface Busines ged Swite an unaute te attack act a crocking (XSS st a user I interface rability ficient value supplied based interface act o cl ious link equently fic web i A success allow the te arbitr in the co ed interface s sensitir I informat I informat B: CVE- 8	ce of Cisc is Smart itches con ithentica iter to iss-site is attack if of the vice. The is due to alidation input be terface of ite. An input be terface of ite. An access a interface is and access a interface is attack iteriace of ite attack iteriace or iteriace or iter	and uld ated, web- of the this the continue to pt the the the the the the the the the th	N/A		H-CIS-S 041119	
sg550xg-48t										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interf Busin Mana allow	nerabilit I manage ace of Ci ess Sma ged Swit an unau te attack	ement sco Sma rt and tches co thentica	ıll uld	N/A		H-CIS-S 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			reques attack system is due prote based interf device explo by per the in malic succe allow perforwith the tare in the tare in the privil could configure communication device the could condition to the tare in	D : CVE-	ry (CSRI ffected ulnerabil fficient (or the we ement n affecte acker co alnerabil g a user of co follow a. A bloit cou cker to rary act lege leve aser. If the inistrative e attackee c cause a ice (DoS an affect	ility CSRF eb- ed ould lity of r a ld ions el of ne er e				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo- condu script again based vulne insuff	nerability I interface Busines ged Swite an unau te attack act a crost cing (XSS st a user I interface rability in ficient va supplied	ce of Cisons Smart aches continued to ss-site of the work. The is due to allidation	and uld ated, veb-	N/A		H-CIS-S 041119	
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	Des	cription	n & CVE I	D	Pato	h	NCIIP	C ID
			web-ba affected attacker vulnera persuad interfact malicio subseque specifict page. A could all execute code in affected access se based in	d device r could be a	e. An I exploit by user of t ick a and access a nterface ssful exp e attack rary scri ntext of face or we brow	this che check the check t				
sg550xg-8f8t			CVE ID 12718	: CVE-	2019-					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulne based n interface Business Manage allow at remote conduct request attack of system, is due to protect based n interface device, exploit by persthe intermalicio success	nanage ce of Ci ss Sma ed Swit n unau attack t a cros forger on an a The v o insuf ions fo nanage ce on a this vu uading erface t us link	ement sco Sma rt and ches co thentica er to ss-site ry (CSRI ffected ulnerabi ficient (or the we ement n affecte acker co ulnerabil g a user to follow a. A	uld ated, ility CSRF eb- ed ould lity of	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
			performation with the tauser has privile could configured comments of the condition of the	D : CVE-	rary act lege leve aser. If the inistrative attacked e e execute c cause a ice (DoS	el of ne ve or				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remote conduscript agains based vulne insuff user-s web-b affect attack vulne persu interf malici subse specif page. could execu code i	nerability interface Busines ged Switt an unaute attack act a crossing (XSS) at a user linterface rability in ficient valued based interface to clipious link equently fic web in A succession the cored interface to clipious link equently fic web in the cored interface to clipious link equently fic web in the cored interface to clipious link equently fic web in the cored interface arbitration the cored interface to clipious link equently fic web in the cored interface arbitration the cored interface arbitration the cored interface arbitration and the cored interface arbitration are arbitration and the cored interface arbitration arbitration are arbitration and the cored interface arbitration arbitration are arbitration and the cored interface arbitration arbitration are arbitration arbitration are arbitration arbitration are arbitration arbitration are arbitration arbitration arbitration arbitration are arbitration arb	ce of Cisons Smart teches continued to ss-site of the way see. The disduction input by terface of the exploit of the access and access anterface of the exploit of the expl	and ald ated, veb- of the this he	N/A		H-CIS-S 041119	
CV Scoring Sca					_					

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			based	s sensiti l informa D : CVE- 8	ation.	ser-				
sx550x-12f										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interface Busin Mana allow remo conductive attack system is due to based interface explosion by performation with a tallow performation with a tallow performation of the tallow configuration of the tallow configuration device allow and device the tallow performation of the tallow configuration of the tallow configuration of the tallow condition of the tallow configuration of the tallow configuration of the tallow condition of the tallow configuration of the tallow condition o	D : CVE-	ement asco Smart and atches continenticater to ass-site ary (CSRI affected allnerability as a user acker continent to follow a continent to follow a continent to acker to array act allege levels as a user. If the inistrative attacker is a cause a continent to affect a cause a continent to a	uld ated, ility CSRF eb- ed uld lity of a ld lity el of ee er ee e e e e e e e e e e e e e e e	N/A		H-CIS-S: 041119	
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	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	4.3	based Small Mana allow remo condi scrip again based vulne insuff user- web- affect attack vulne persu interf malic subse speci page. could execu code affect attack vulne persu interf malic subse speci page.	nerability I all all all all all all all all all al	ce of Cis ss Smart tches co uthentica cer to ss-site S) attack cof the v ce. The is due to alidation d input b terface o ce. An d exploit by user of t lick a c and access a nterface ssful exp ne attack rary scri ontext of face or ve brow ation.	co and uld ated, veb- o o o o o o o o o o o o o o o o o o o	N/A		H-CIS-S 041119	
sx550x-16ft											
Cross-Site Request Forgery (CSRF)	16-	10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site				N/A		H-CIS-S 041119	
CV Scoring Sca	le	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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			attack system is due prote based interfedevice explosion by pethe immalice succes allow perfowith the tauser hyprivile could configure communication devices attacks.	D : CVE-	ffected ulnerabil fficient (or the we ement in affecte acker co ulnerabil g a user o co follow a. A bloit cou cker to rary act lege leve aser. If th inistrativ e attacke c cause a ice (DoS an affect	ility CSRF eb- ed ould lity of a ld ions el of ne er e				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s	nerabilit l interface Busines ged Switt an unaute attack act a crost cing (XSS st a user l interface rability i ficient va supplied pased int	ce of Cisons Smart teches continued to ss-site of the way. The is due to lidation input by	and uld ated, web-	N/A		H-CIS-S 041119	
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	D	escription	n & CVE II	D	Pat	ch	NCIIP	CID
			affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browserbased information. CVE ID: CVE-2019-12718							
sx550x-24										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	based interf Busin Mana allow remore conductive attack system is due prote based interf device explosion by pethe in malic succes	nerability I manage Face of Ci Less Smar ged Switt an unau te attack act a cros est forger k on an a m. The vo e to insuf ctions fo I manage it this vu rsuading aterface t ious link ssful exp	ement sco Sma rt and ches con thentica er to ss-site ry (CSRF ffected ulnerabil fficient C r the we ement n affecte acker co dlnerabil g a user o to follow to A bloit cou	all uld ated, ility SSRF eb- ed uld aity of	N/A		H-CIS-S 041119	
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	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
			with the tauser he privil could configure communication devices	D : CVE-	lege levenser. If the nistrative attacker executed cause a cause a cause an affect	el of ne ve er e				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulne based Small Mana allow remo conduscript again based vulne insuff users web-laffect attack vulne persuinterf malic subset specific page. could execut code affect	nerability language of Swite an unaute attack act a crossing (XSS) at a user language of the device	the of Cisons Smart teches contithenticated to ss-site of the way the continuation of the continua	and uld ated, veb- of the this he cloit ter to pt the	N/A		H-CIS-S 041119	
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
			based information.		
			CVE ID : CVE-2019- 12718		
sx550x-24f					
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. CVE ID: CVE-2019-12636	N/A	H-CIS-SX55- 041119/1432

Weakness	Publish Date	CVSS	Description & CVE ID				Pato	:h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remore condustrictions of the second secon	l interface Busines ged Swi an unau te attack act a cro cing (XSS st a user l interface rability ficient value coased in ed device coased in ed device rability ading a face to cla ious link equently fic web i A succe allow the te arbite in the co ed inter s sensiti l inform D: CVE	ss-site c) attack cof the vece. The dis due to didation dinput b terface of ee. An dexploit by user of t dick a access a nterface ssful exp ne attack cary scri ontext of face or ve brow ation.	and uld ated, web- of the this the coloit ser to pt the the	N/A		H-CIS-S 041119	
sx550x-24ft										
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A vulnerability in the web- based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site				N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			attack system is due prote based interfedevice explosion by pethe immalice succes allow perfowith the tauser hyprivile could configure communication devices attacks.	D : CVE-	ffected ulnerabil fficient (or the we ement in affecte acker co ulnerabil g a user o co follow a. A bloit cou cker to rary act lege leve aser. If th inistrativ e attacke c cause a ice (DoS an affect	ility CSRF eb- ed ould lity of a ld ions el of ne er e				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s	nerabilit l interface Busines ged Switt an unaute attack act a crost cing (XSS st a user l interface rability i ficient va supplied pased int	ce of Cisons Smart teches continued to ss-site of the way. The is due to lidation input by	and uld ated, web-	N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718 A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches 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 for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could	Weakness	Publish Date	CVSS	Des	Description & CVE ID				h	NCIIP	CID
SX550x-52 A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could				attacker vulnera persuad interface malicion subseque specifice page. A could all execute code in affected access s	c could bility he to clius link uently web in succession the could be arbitrathe arbitrathe could be arbitrathe could be arbitrathe could be arbitrathe could be arbitrathe a	l exploit by user of t ick a and access a aterface esful exp e attack ary scri- ntext of face or ve brow	he loit er to pt the				
Cross-Site Request Forgery (CSRF) 16-10-2019 6.8 A vulnerability in the webbased management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could	cvEEAv.E2			CVE ID							
based management interface of Cisco Small Business Smart and Managed Switches 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 for the webbased management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could	32300 32			A vulne	rabilit	y in the	web-				
allow the attacker to	Request Forgery	16-10-2019	6.8	interface Busines Manage allow an remote conduct request attack of system. is due to protect based m interface device. exploit by perso the inter malicion success	based management interface of Cisco Small Business Smart and Managed Switches 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 for the web- based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A						

(CVSS)

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pat	ch	NCIIP	CID
			with the tauser he privil could configured communication devices	D : CVE-	lege levenser. If the nistrative attacker executed cause a cause a cause an affect	el of ne ve er e				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remore conduscript again based vulne insuff user-s web-l affect attack vulne persu interf malic subse specif page. could execu code i	nerability interface an unaute attack act a crossing (XSS) st a user interface rability in ite attack act a could be act a could be act a could be act act a could be act	the of Cisons Smart teches contithenticated to ss-site of the way to alidation input by the certain access and access access and access and access and access access and access access access and access ac	and uld ated, web- of the this he could be the country	N/A		H-CIS-S 041119	
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	D	escription	a & CVE II	D	Pato	h	NCIIP	CID
				l informa D : CVE- 8						
spa112										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interf Series Adapt allow remore condustript vulne insuff user-s web-hinterf softw could vulne persua craf exploattack arbitr conteinterf sensit inform	nerability an author at attack act cross and attack act cross and attack act cross and attack act cross and attack act act and attack act act and attack act	ement sco SPA Telepho As) coul enticate er to -site cks. The cks. The didation input b anagemo e affecto attacker this by user to o A succe allow th ecute ot code i affected ccess wser-ba	100 one d d, of y the ent ed click ssful e	N/A		H-CIS-S 041119	
Information Exposure	16-10-2019	4	A vulnerability in the web- based management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to view the contents of arbitrary			100 one d d,	N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	lle 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	a & CVE II	D	Pato	:h	NCIIP	CID
			The vimpro in the mana attack vulne crafte web-linterf device exploattack conte on the result of sen	on an affectulnerability of web-based managed	lity is du at validated interfaced exploit exploit exploit exploit anagement affecter essful allow th crieve th bitrary f possibly e disclo formation	e. An this ng a ent d				
			1270	D : CVE- 4 nerabilit		woh-				
Information Exposure	16-10-2019	4	based interf Series Adapt allow removes an aff vulne unsaf crede could vulne portion mana an aff succe allow acces crede crede	manage ace of Ci s Analog ters (ATA an authorie attack cive information of the property of the attack s adminintials an elevated	ement sco SPA Telepho As) coulcenticate er to accommation vice. The s due to n attack this by viewif e web-be interface vice. A bloit coun cker to strative d poten	100 one d d, cess on e er er ld dsed dtially	N/A		H-CIS-S 041119	
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
			reusing stolen credentials on the affected device. CVE ID: CVE-2019- 12708		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15240	N/A	H-CIS-SPA1- 041119/1441
Improper Restriction of Operations within the Bounds of a Memory	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code	N/A	H-CIS-SPA1- 041119/1442
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	D	escription	ı & CVE II	D	Pato	:h	NCIIP	CID
Buffer			The v to impuser-s web-l interf could vulne authe based interf crafte affect succe allow execu with o Note: mana enabl CVE I	elevated ulnerabited proper visupplied pased marage and a certained requested devices ful experience arbitrate arbitrate arbitrate arbitrate devated The well gement is ed by de D: CVE-1	lities are alidation input to anagement these is by g to the verment sending sts to an e. A bloit coucker to privilegobased interface fault.	e due n of the ent web-				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due				N/A		H-CIS-S 041119	
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	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
			succe allow execu with Note: mana enabl CVE I 1524	ed devices saful expected arbitrated. The well gement ed by de ED: CVE-2	oloit cou cker to cary cod privileg o-based interfact fault. 2019-	e ges. e is				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adap allow adjace executive with a to improve the could will be auther affect succe allow executive with a to improve the could with a to interfect affect succe allow executive with a total analogous manalogous analogous analogous manalogous analogous an	SPA100 og Teleph ters (ATA an auth ent attace te arbitr elevated rulnerabi proper v supplied based ma face. An a exploit enticating d manage face and ed reques sed device ested device strabilitie the atta te arbitr elevated The well ed by de to : CVE-	Series none As) coul enticate cker to rary cod privileg alidatio input to anagement acker these is by g to the sement sending sts to an e. A cloit courary cod privileg obased interface fault.	d d, e ges. e due n of o the ent ld e ges.	N/A		H-CIS-S 041119	
Improper	16-10-2019	5.2	Multiple vulnerabilities in			N/A		H-CIS-S	PA1-	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
Restriction of Operations within the Bounds of a Memory Buffer			Analo Adapt allow adjace execution with a to impuser such authorized authorized affect succe allow execution with a Note: manalenabl CVE I 1524		none As) coulcenticate elker to rary code privileg elities are alidation input to an agement sending sts to an e. A coloit courary code privileg co-based interface fault. 2019-	d, e ges. e due n of o the ent ld e ges. e is			041119	/1445
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapt allow adjace execu with o The v to impuser-s web-l	ple vulne SPA100 og Teleph ters (ATA an authe ent attac te arbitr elevated ulnerabi proper v supplied based ma	Series none As) coulcenticate eker to cary code privileg elities are calidation input to	d d, e ees. e due n of o the	N/A		H-CIS-S 041119	
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	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			vulne auther based interfer crafted affect succe allow execution with a Note: mana enable	exploit rabilities rabilities rabilities rate and ed reques ed device ssful expected the attacte arbitral elevated. The well gement sed by de D: CVE-5	s by g to the sement sending sts to an e. A bloit cou cker to privileg b-based interface fault.	ld e es.				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapt allow adjace execu with o The v to imp user-s web-l interf could vulne authe based interf crafte affect succe allow execu with o	ple vulne SPA100 og Teleph ters (ATA an authorent attace te arbitroper volunerabilities and exploit frabilities and ed reques ed device ssful expented attace arbitroper the attace arbitroper the attace arbitroper the well-wated The well-wated arbitroper the well-wated arbitroper the attace arbitroper the attace arbitroper the well-wated The well-wated spans arbitroper the attace arbitroper the well-wated arbitroper the well-wated spans arbitroper the wated spans arbitroper the well-wated spans arbitroper the wated spans arbitroper the	Series none As) coul enticate ker to rary code privileg lities ar alidation input to anagement acker these is by get to the resending sets to an e. A coloit courary code privileg	d d, e ees. e due n of o the ent ld	N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	lle 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 interface is enabled by default. CVE ID: CVE-2019- 15246		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code with elevated privileges. The vulnerabilities are due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit these vulnerabilities by authenticating to the web-based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019-15247	N/A	H-CIS-SPA1- 041119/1448
Improper Restriction of Operations within the Bounds of a Memory	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, adjacent attacker to execute arbitrary code	N/A	H-CIS-SPA1- 041119/1449
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	D	escriptio	n & CVE I	D	Pa	atch	NCIIP	C ID
Buffer			The verto impuser- web-linterificould vulner authority crafter affect successful allow executive with a Note: manalenable	elevated rulnerab proper versupplied based managed exploit exp	ilities ar validatio linput to anagemo attacker these s by g to the ement sending sts to an ecker to cary cod privileg b-based interface afault.	e due n of o the ent web-				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adap allow adjac execu with to im user- web- interf could vulne authe based interf	ple vuln SPA100 og Telepl ters (AT an auth ent attac ite arbiti elevated rulnerab proper v supplied based m face. An a exploit erabilitie enticatin d manage face and ed reque	Series hone As) coul enticate cker to rary cod privileg ilities ar validatio l input to anagement these s by g to the sending	d d, e ges. e due n of o the ent	N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6					7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pato	:h	NCIIP	C ID
			succe allow execu with Note: mana enabl CVE I 1524	ed devices saful expected arbitrated. The well ed by de ED: CVE-19	oloit cou cker to cary cod privileg o-based interfact fault. 2019-	e ges. e is				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adaptallow adjacted executives with a could vulne auther based interference allow executives with a could with a could with a could with a could be a cou	SPA100 og Teleph ters (ATA an auth ent attace te arbitr elevated rulnerabi proper v supplied based ma face. An a exploit enticating d manage face and ed reques sed device ested device strabilitie the atta te arbitr elevated The well ed by de to : CVE-	Series none As) coul enticate cker to rary cod privileg ditties ar alidation input to anagement acker these is by get to the sending sets to an e. A coloit courary cod privileg obased interface fault.	d d, e ges. e due n of o the ent ld e ges.	N/A		H-CIS-S 041119	
Improper	16-10-2019	5.2	Multiple vulnerabilities in			N/A		H-CIS-S	PA1-	
CV Scoring Sca (CVSS)	o-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	ch	NCIIP	CID
Restriction of Operations within the Bounds of a Memory Buffer			Analo Adapt allow adjace execution with a to impuser such authorized and authorized affect succe allow execution with a total enable CVE I 1525		As) coulenticate eker to cary code privileged input to an agement sending sts to an e. A coloit coucker to cary code privileged b-based interface fault.	d, e ges. e due n of o the ent ld e ges. e is			041119	/1452
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-10-2019	5.2	Cisco Analo Adapt allow adjace execu with o The v to impuser-s web-l	ple vulne SPA100 og Teleph ters (ATA an authe ent attace te arbitr elevated rulnerabi proper v supplied based ma	Series none As) coulenticate cker to cary code privilegilities are alidation anagements.	d d, e ges. e due n of o the ent	N/A		H-CIS-S 041119	
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
			could exploit these vulnerabilities by authenticating to the web- based management interface and sending crafted requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. CVE ID: CVE-2019- 15252		
Information Exposure	16-10-2019	4	A vulnerability in the webbased management interface of Cisco SPA100 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper restrictions on configuration information. An attacker could exploit this vulnerability by sending a request to an affected device through the web-based management interface. A successful exploit could allow the attacker to return running configuration information that could also include sensitive information.	N/A	H-CIS-SPA1- 041119/1454

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
			CVE I 1525	D : CVE- 7	2019-					
Improper Input Validation	16-10-2019	6.8	based interf Series Adaptallow remo denia on an vulne improuser-the was attack vulne crafte web-linterf device exploattack device requirements of the control of the contro	nerabilited manage face of Cities Analog ters (AT) an author terms affected rability oper valing supplied reduced requestance of an eace of an	ement isco SPA Telepho As) coul enticate cer to ca ice cond device. is due to dation o reques d interfac d exploit by sendi st to the anagemo affecte cessful allow th use the respon nual for recov	one d d, use a lition The of ts to e. An this ing a ent d e ding,	N/A		H-CIS-S 041119	
ngips_virtua	l_appliance									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the w mana Cisco Mana (FMC authe attacl cross	ple vulngeb-based gement Firepow gement could a could a cer to co-site scritcated a gainst	d interfac ver Center allow an I, remote nduct a	e of	N/A		H-CIS-N 041119	
CV Scoring Sca (CVSS)	o-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	h	NCIIP	C ID
			web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268							
					2019-					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attack cross attack web-linterf vulne insuff user-sweb-linterf could vulne	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the					H-CIS-N 041119	
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	D	escription	n & CVE I	D	Pato	h	NCIIP	CID
			could execu- code interf sensi- inform CVE I 1526	nerabilit	ne attack rary scri ntext of ccess wser-ba 2019-	er to pt the sed				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	interf Firep Center an un remo condu script again based interf vulne insuff user- web-l interf could vulne persu interf link. A could execu- code interf sensit inform	I manage face of Ciower Mater (FMC) authentificate attack face. The trability is face. An attack face to classed mater ability is face to classed mater arbitrate arbitrate arbitrate arbitrate arbitrate arbitrate arbitrate. An attack of ace or active, brown atton.	isco anageme could al icated, er to ss-site b) attack of the v ement is due to alidation input b anageme attacker this by user of t ick a cra sful expl ary scri ntext of ccess wser-ba	veb- of y the ent che afted oit ser to pt	N/A		H-CIS-N 041119	
firepower_ap	ppliance_8390									
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	D	escription	ո & CVE II	D	Pato	:h	NCIIP	CID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attack cross-attack web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuinterf sensit inform	ple vulne eb-based gement in the contact of a success allow the tearbitre in the contact of a success allow the arbitre in the arbitre in the contact of a success allow the arbitre in the contact of a success allow the arbitre in the contact of a succe	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement input by anagement attacker these is by user of t ick a cra sful expl are attack vary scri- ntext of ccess wser-bas	e of SSS) of the ent e to of y the ent the oft the to the to	N/A		H-CIS-F 041119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management				N/A		H-CIS-F 041119	
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
			interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019- 15269		
firepower_ap	ppliance_8270				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the	N/A	H-CIS-FIRE- 041119/1461

2-3

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizati on of Input During Web Page Sensitive, browser-based management interface or acces wulnerabilities by persuading a user of the interface of cilck a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface. An attacker to excess the scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269	Weakness	Publish Date	cvss	Descriptio	n & CVE II)	Pato	h	NCIIP	C ID
the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of User-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-				link. A success could allow to execute arbit code in the continue interface or a sensitive, browninformation. CVE ID: CVE	esful explo he attack rary scrip ontext of ccess wser-bas	oit er to ot the				
	Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	3.5	the web-base management Cisco Firepox Management (FMC) could authenticated attacker to co cross-site scrattack agains web-based minterface. The vulnerabilitie insufficient vuser-supplied web-based minterface. An could exploit vulnerabilitie persuading a interface to could allow the execute arbiticode in the cointerface or a sensitive, browinformation. CVE ID: CVE	interface ver Center allow an d, remote onduct a ipting (X) t a user of an agement attacker these es by user of the attack rary scrip ontext of access owser-base ver-base ver	SS) f the ent to of the ent ne fted oit er to ot the	N/A			

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firepower_m	anagement_ce	nter_4	500		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268	N/A	H-CIS-FIRE- 041119/1463
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS)	N/A	H-CIS-FIRE- 041119/1464

Weakness	Publish Date	CVSS	Description & CVE ID				Pato	h	NCIIP	C ID
			attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15269							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interf Firep Center an un remore condustript again based interf vulne insuff user-web-linterf could	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by					H-CIS-F 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			link. A could execu code interf sensit inform	A success allow the arbitroin the conface or active, brownation. D: CVE-	wser-ba	oit er to pt the				
firepower_ap	pliance_8250		<u>, </u>							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-web-linterf could vulne persuinterf link. A could execute code interf sensitinform	eb-base gement Firepow gement (a) could a conticated for the conticate	interfactiver Center Allow an I, remote anduct a ipting (X a user of an agement attacker these attacker of the attacker attacker acray scripntext of access wser-bar	e of (SS) of the ent e to of y the ent che afted loit ser to pt the	N/A		H-CIS-F 041119	
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	Pul	blish Date	e CVSS	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
				1526	8						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterfi vulne insuffi user-sweb-linterfi could vulne persu interfi link. A could execut code sinterfi sensiti informatical control of the could execut code sinterfi sensiti informatical control of the could execut code sinterfi sensiti informatical control of the could execut code sinterfi sensiti informatical control of the could execut code sinterfi sensiti informatical control of the control	ple vulne eb-base gement Firepow gement) could a nticated ker to co site scri k against based ma face. The rabilitie ficient va supplied based ma face. An a exploit rabilitie ading a face to cl A success allow th te arbitr in the co face or ac cive, brow nation. D: CVE- 9	interface ver Center Illow an , remote anduct a pting (X a user of anagement input be anagement input be are attacker interest of coessi interest	e of SSS) of the ent e to of y the ent he afted oit aer to pt the	N/A		H-CIS-F 041119	
firepower_m	anag	gement_	center_4	600							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a				N/A		H-CIS-F 041119	
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	3-4	4-5	4-5 5-6		7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pato	:h	NCIIP	CID
			attack web-l interf vulne insuff user-s web-l interf could vulne persu interf link. A could execu code s interf sensit inform	rabilities ace. The rabilities ased marked marked marked marked marked marked marked ace. An ace ace to classed the arbitrin the contact of ace or active, brown ation. D: CVE-8	a user of an agement of the se of th	e to of y the ent he ofted oit ter to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-sweb-linterf could	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by					H-CIS-F 041119	
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
			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 access sensitive, browser-based information. CVE ID: CVE-2019-15269		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the webbased management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased management interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. 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 access sensitive, browser-based information. CVE ID: CVE-2019-	N/A	H-CIS-FIRE- 041119/1470

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIII	PC ID
			1527	0						
firepower_ap	ppliance_8120									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268				N/A		H-CIS-F 041119	
Improper Neutralizati on of Input			Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a							
During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5					N/A		H-CIS-F 041119	
CV Scoring Sca (CVSS)	o-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
			cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-		
C	1: 0250		15269		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker	N/A	H-CIS-FIRE- 041119/1473

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities 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 access sensitive, browser-based information. CVE ID: CVE-2019-15268		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities 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 access sensitive, browser-based	N/A	H-CIS-FIRE- 041119/1474

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pate	:h	NCIIF	PC ID
			infori	nation.						
			CVE I 1526	D : CVE- 9	2019-					
firepower_ap	pliance_8140									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC auther attack cross attack web-linterf vulne insuff user-sweb-linterf could vulne persuinterf link. A could execut code interf sensitinform CVE I 1526		dinterface ver Center allow an , remote nduct a pting (X a user of anageme attacker these s by user of t ick a cra sful expl ne attack cary scri ntext of ccess wser-ba	e of (SS) of the ent e to of ythe ent the oft the sed	N/A		H-CIS-F 041119	
Improper Neutralizati on of Input During Web	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower				N/A		H-CIS-F 041119	
Page Generation			Management Center (FMC) could allow an							
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	Des	scriptio	n & CVE I	D	Pate	ch	NCIIP	CID
('Cross-site Scripting')			authen attacke cross-s attack a web-ba interfacture could e vulnera insufficial interfacture persuaci interfacture facture could a execute code in interfacture facture facture code in interfacture facture facture facture facture code in interfacture facture fact	ticated or to co ite scripagainst ased made. The abilitie dised made. An abilitie ding a ce to classification of the core or action.	tremote a user of an agementacker of these attacker of the att	esto esto of the ent eto of y the ent che afted oit ser to pt				
firepower_ap	pliance_7050									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the well manage Cisco F Manage (FMC) authen attacke cross-s attack a web-ba interfactulnera insuffic	b-based ement could a ticated er to could against against ce. The abilitie cient va	interfacter Ver Center Allow an I, remote Induct a Ipting (X I a user of	e of (SS) of the ent e to	N/A		H-CIS-F 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
			interf could vulne persu interf link. A could execu code i interf sensit inform	pased marace. An a exploit frabilities ading a frace to class allow that arbitrate arbitrate or ace or active, brownation. D: CVE-8	attacker these s by user of t ick a cra sful expl ae attack rary scri ntext of ccess wser-ba	he fted oit er to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attackers attackers web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could execuing code in the could execuing the could execuing the could execuing the code in the could execuing the code in the could execuing the code in the code i	ple vulne eb-based gement of Firepow gement of could a nticated act to consiste scri- cagainst based managed ace. The rabilities ace. An a exploit of ace to classifies allow the te arbitr in the consister ace	dinterface ver Center Illow an , remote nduct a pting (X a user of anagement is a user of anagement input be anagement input be anagement input input be anagement input in	es of established site of the ent established site of the	N/A		H-CIS-F 041119	
	le 0.1									

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pato	h	NCIIP	CID
			infor	cive, brov nation. D : CVE- o		sed				
firenewer ar	pliance_8260		1520	9						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wimana Cisco Mana (FMC) auther attackers attackers web-kinterf vulne insuff user-sweb-kinterf could vulne persuinterf link. A could	ple vulne eb-based gement (Firepow gement () could a nticated cer to con- site scri a against cased ma face. The rabilities ace. An a exploit (rabilities ading a u face to cli	dinterface ver Center llow an , remote nduct a pting (X a user of anagement in a user of anagement in put by anagement it a crass stacker these is by user of t ick a crass ful expl	e of (SS) of the ent e to of y the ent the ifted oit cer to	N/A		H-CIS-F 041119	
Improper			code interf sensit inform CVE I 1526		ntext of ccess wser-ba 2019-	the sed				
Improper Neutralizati on of Input During Web Page	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center				N/A		H-CIS-F 041119	
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	De	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
Generation ('Cross-site Scripting')			(FMC) auther attack cross-attack web-binterface web-binterface could vulner persuinterface could execute code in interface interface could execute code interface interface interface interface code interface information informatical code in interface code in interface code in interface code in interface code in interface code code code code code code code co	could a nticated art to consite scrip against ace. The rabilitie ace. An ace ace to classed mace to classed mace at a ce arbiting a ace to classed ace to classed mace ace to classed mace ace or ace or ace or ace or ace or ace or acive, brownation. D: CVE-	allow an l, remote a tauser of a user of a user of the attacker of the attacke	esss) of the ent e to of y the ent the afted oit cer to pt the				
firepower_ap	pliance_8360									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	the wo	eb-base gement Firepow gement could a nticated ser to consite scrite scrite against pased mace. The rabilitie	interfactiver Center Allow an I, remote Induct a Ipting (X I a user of	e of (SS) of the ent e to	N/A		H-CIS-F 041119	
CV Scoring Sca	le 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	D	escription	n & CVE II	D	Pato	:h	NCIIP	C ID
			web-linterf could vulne persu interf link. A could execu code interf sensit inform	supplied based made. An a exploit for a carbilities ading a success allow the arbitrin the contact or active, brown ation. D: CVE-8	anagemonttacker these s by user of t ick a cra sful expl ne attack eary scri ntext of ccess wser-ba	he fted oit eer to pt the				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multithe we mana Cisco Mana (FMC) auther attacked interfered web-kinterfered vulne insuffered vulne persuinterfered vulne vu	ple vulne eb-based gement if Firepow gement if Could a	interface ver Center Illow an , remote anduct a pting (X a user of anagement is are dural input by anagement anagement input by anagement input by anagement input by anagement input by anagement attacker these is by user of t ick a cra sful expl attacker	e of esss) of the ent e to of y the ent he ent	N/A		H-CIS-F 041119	
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	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	C ID
			sensi	face or active, bromation.		sed				
			CVE I 1526	D : CVE- 9	2019-					
firepower_ma	anagement_c	enter								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	based interfacent information interfacent interfacent interfacent information interfacent	nerability I manage face of Ci ower Ma er (FMC) authent te attack act a cro ting (XSS st a user I manage face. The erability ficient va supplied based ma face. An a exploit erability ading a face to cl A success allow the active, bro mation. CD: CVE- CO	ement isco anageme could a icated, aer to ss-site 6) attack of the v ement is due to alidation linput b anageme attacker this by user of t ick a cra sful expl aer attack ary scri ontext of ccess wser-ba	ent llow veb- on of y the ent che afted loit ger to pt the	N/A		H-CIS-F 041119	
webex_room_	_kit_mini									
Incorrect Default	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence				N/A		H-CIS-V 041119	
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	Descr	iption & CVE II)	Pato	h	NCIIP	C ID
Permissions			(CE) Soft an auther attacker to the /root affected of vulnerable improper assignment could exp vulnerable as the remand writite /root directed of	ility by loggin notesupport ng files to the ectory of an	llow l to an er ng in user				
sg300-28pp									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based interface malicious subseque	a cross-site (XSS) attack user of the werface. The allity is due to nt validation plied input by ed interface of levice. An could exploit allity by a user of to click a	of the this	N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3	-4 4-5 944	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			could execu code affect acces based	A succe allow the arbitrin the cored inters sensitill inform D: CVE-8	ne attack cary scri ontext of face or ve brow ation.	ter to pt the				
sg300-28sfp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability l interface Busines ged Swite an unaute attack act a crooting (XSS st a user l interface rability ficient variability ficient variability adding a face to clain act a crooting line and device act a crooting to the crooting act and the crooting act	ce of Ciscos Smart tches conthenticater to ss-site S) attack to find the voce. The hiddetion of the voce and exploit to the stand access a context of face or ve brown ation.	and uld ated, web- of the this the coloit ser to pt the the	N/A		H-CIS-S 041119	
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	D	escription	a & CVE II	D	Pate	ch	NCIIP	CID
			1271	8						
sg300-52										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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- 12718				N/A		H-CIS-S 041119	
sg300-52mp							I			
Improper Neutralizati on of Input During Web Page Generation	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to				N/A		H-CIS-S 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
('Cross-site Scripting')			script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	act a cro ting (XSS st a user d interface erability ficient va supplied based in ted device ker could erability lading a face to cla clous link equently fic web i A succes allow the arbite in the could ted inter s sensiti d inform ID: CVE- 8	s) attack ce. The is due to alidation d input b terface of ee. An d exploit by user of t lick a access a nterface ssful exp ne attack rary scri ontext of face or ve brow ation.	veb- of of y the of the				
sg300-52p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-	nerability an unaute attack uct a croting (XSS st a user a linterfaction to the conting to the continuous	ce of Ciscs Smart tches conthenticater to ss-site of the voce. The is due to alidation the put by the control of the total input by the control of the control of the total input by the control of the	co and uld ated, veb-	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			attacl vulne persu interf malic subse specia page. could execu code affect acces	ted device of the control of the con	d exploit by user of t ick a and access a nterface ssful exp ne attack cary scri ontext of face or	he oloit er to pt the				
				D : CVE						
sf500-24									T	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse	nerability I interface Busines ged Swi an unau te attack uct a cro ting (XSS st a user I interface rability ficient va supplied based in ted device erability rading a face to cl ious link equently fic web i	ce of Ciso is Smart tches con athentica ter to ss-site S) attack of the vice. The alidation diduction dinput b terface of te. An didexploit by user of the ick a and access a	and ald ated, web- of the athis the	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			could execu code affect acces based	A succestallow the arbitration the content of the c	ne attack cary scri intext of face or ve brow ation.	ter to pt the				
sf500-24mp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability I interface Busines ged Switter an unaute attack act a crooting (XSS st a user I interface rability ficient variability adding a face to clain and act a crooting interface rability adding a face to clain act act a clain act	ce of Cisc is Smart itches co athentica iter to iss-site of the vice. The is due to alidation dinput b terface of te. An diexploit by user of t ick a access a nterface is and access a nterface is attack cary scri- ontext of face or ve brow ation.	and ald ated, web- of the athis the alloit ter to pt the	N/A		H-CIS-S 041119	
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	1	NCIIP	C ID
			12718				
sf500-24p							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718			H-CIS-SI 041119	
sf500-48							
Improper Neutralizati on of Input During Web Page Generation	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to	N/A		H-CIS-SI 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6 950	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
('Cross-site Scripting')			script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	act a cro ting (XSS st a user d interface rability ficient var supplied based in ted device rability ading a face to cl ious link equently fic web i A succes allow the te arbitr in the co ted inter s sensiti d informatic ID: CVE- 8	s) attack ce. The is due to alidation d input b terface of ee. An d exploit by user of t lick a access a nterface ssful exp ne attack rary scri ontext of face or ve brow ation.	veb- on of y the of the				
sf500-48mp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-	nerabilited interface Busines ged Swite an unaute attack uct a crooting (XSS st a user dinterface rability ficient valued based in	ce of Ciscs Smart tches conthenticater to ss-site of the voce. The is due to alidation this contract to the voce the is due to alidation to the voce.	co and uld ated, veb-	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	escription	a & CVE II	D	Pat	ch	NCIIP	CID
			attack vulnes persu interfa malici subse specif page. could execu code i affecte access based	ed device a could rability be adding a uace to clistons link quently ic web in A success allow the arbitren the could interfes sensitive information : CVE-8	l exploit by user of t ick a and access a aterface sful exp e attack ary scrip ntext of face or ve brow	he loit er to pt the				
sf500-48p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Manag allow remot condu script agains based vulnes insuff user-s web-b affecte attack vulnes persu interf malici subse	nerability interface Busines ged Switten an unauste attack act a crossing (XSS) at a user interface rability is icient valued devices could rability be adding a unace to climble fous link quently ic web in the could be accepted to the could be ac	te of Ciscos Smart ches conthenticater to ss-site attack of the way. The state to lidation input by terface on the control of	of the this	N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	o-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			could execu code affect acces based	A succestallow that arbitration the content of the	ne attack cary scri intext of face or ve brow ation.	ter to pt the				
sg500-28										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability I interface Busines ged Swir an unau te attack act a cro cing (XSS st a user I interface rability ficient va supplied based in red device act o cl ious link equently fic web i A succes allow the act arbitr in the co red interface in the co red interface by a succes allow the color of the color act of	ce of Cisc is Smart itches co athentica iter to iss-site of the vice. The is due to alidation dinput b terface of te. An diexploit by user of t ick a access a nterface is and access a nterface is attack cary scri- ontext of face or ve brow ation.	and uld ated, web- of the this the continue to pt the the the the the the the the the th	N/A		H-CIS-S 041119	
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 D	Date	cvss	D	escription	n & CVE I	D	Р	atch	NCIIP	CID
				1271	8						
sg500-28mpj	p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-20	019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability in the could arbitry in the could arbitr	the of Cisc is Smart thentical ter to is s-site of the vice. The is due to didation input b terface of e. An d exploit by user of t ick a access a nterface ssful exp ie attack cary scri intext of face or ve brow ation.	and uld ated, web- of the this he could be the country	N/A		H-CIS-S 041119	
sg500-28p Improper				A vulnerability in the web-			wob				
Neutralizati on of Input During Web Page Generation	16-10-20	019	4.3	based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to				N/A		H-CIS-S 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
('Cross-site Scripting')			condi- scripi again based vulne insufi user- web- affect attack vulne persu interi malic subse speci page. could execu code affect acces based	uct a cro ting (XSS ast a user d interface erability ficient va supplied based in ted device ker could erability lading a face to cle clous link equently fic web i A succe al allow the late arbite in the could ted inter es sensiti d information.	ss-site s) attack cof the v ce. The is due to alidation d input b terface o ce. An d exploit by user of t lick a c and access a nterface ssful exp ne attack rary scri ontext of face or ve brow ation.	veb- of of y the of the cathis che cathis che defined the cathis che				
sg500-28pp										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condi scrip again based vulne insuff user-	nerabilited interface land switch a unaute attack uct a croping (XSS ast a user land interface rability ficient vasupplied based in	ce of Cises Smart tches conthenticater to ss-site of the voce. The is due to alidation the input be seen to the total to t	and uld ated, web-	N/A		H-CIS-S 041119	
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718 Sg500-52 A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface ### CIS-SG50-041119/1500	Weakness	Publish Date	cvss	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
sg500-52 A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a				attack vulne persu interf malic subse specif page. could execu code i	rability rability ading a face to cl ious link equently fic web i A succes allow th te arbits in the co ed inter s sensiti	d exploit by user of t ick a and access a nterface ssful exp ne attack cary scri ontext of face or	he cloit eer to pt the				
A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches 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 ('Cross-site Scripting') 4.3 4.3 H-CIS-SG50- 041119/1500 H-CIS-SG50- 041119/1500 affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a	sg500-52			CVE I	D : CVE-						
	Improper Neutralizati on of Input During Web Page Generation ('Cross-site	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s web-l affect attack vulne persu interf malic subse	l interface Busines ged Swith an unaute attack act a crooking (XSS) st a user l interface rability ficient value cased in ed device act could rability ading a face to cl ious link equently	ce of Cisons Smart teches continued to see to see to see the continued to the central terface of tentral terface of the central terface o	and ald ated, web- of ythe of the athis	N/A			

(CVSS)

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			could execu code affect acces based	A succe allow the arbitration the content of the co	ne attack cary scri ontext of face or ve brow ation.	ter to pt the				
sg500-52mp			•							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	nerability I interface I Busines I ged Swi I an unau I te attack I uct a cro I interface I	ce of Ciscos Smart tches conthenticater to ss-site S) attack to find the voce. The hiddetion of the voce and exploit to the stand access a mand access a man	and uld ated, web- of the this the coloit ser to pt the the	N/A		H-CIS-S 041119	
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	Publisl	h Date	cvss	D	escription	n & CVE I	D	ı	Patch	NCIII	PC ID
				1271	8						
sg500-52p											
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-	2019	4.3	based Small Mana allow remore condu- script again, based vulne insuff user-s web-laffect attack vulne persu- interf malic subse specifi page, could execu- code i affect attack vulne interf malic subse specifi page, could execu- code i affect subse specifi page, could execu- code i affect subse specifi page, could execu- code i affect access page, could execu- code i access page, code i access page, access page, access page, access page, access page, access access access page, access page, access page, access page, access page, access page, access page, access page, access page, access page, access page, access page, access page, access acces acces access access access access acces access acces access access acces acces acces acce	nerability lands lines and unaute attack act a crossing (XSS st a user linterfactors ability lands link adding a lands link ad	the of Cisc is Smart thentical ter to is s-site of the vice. The is due to didation input b terface of e. An d exploit by user of t ick a access a nterface ssful exp ie attack cary scri intext of face or ve brow ation.	and uld ated, web- of the this he could be the country	N/A		H-CIS-S 041119	
sg500-52pp							I				
Improper Neutralizati on of Input During Web Page Generation	16-10-	2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to				N/A		H-CIS-S 041119	
CV Scoring Scal	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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	PC ID
('Cross-site Scripting')			conduscript again based vulne insuff user-s web-laffect attack vulne persu interf malic subse specific page. could execu code affect acces based	act a cro ting (XSS st a user d interface rability ficient va supplied based in ted device act could rability face to cl ious linl equently fic web i A succe allow the te arbite in the could ted inter s sensiti d inform	ss-site s) attack cof the v ce. The is due to alidation d input b terface o ce. An d exploit by user of t ick a c and access a nterface ssful exp ne attack cary scri ontext of face or ve brow ation.	veb- of of y the of the cathis che oloit ser to pt other of the				
sg500x-24										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user-s	nerabilit l interface Busines ged Swi an unau te attack uct a cro ting (XSS st a user l interface rability ficient va supplied based in	ce of Ciscs Smart tches conthenticater to ss-site of the voce. The is due to alidation this put by the control of the total input by the control of the control of the total of the total of the control	and uld ated, web-	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE II	D	Pato	h	NCIIP	CID
			attack vulne persu interf malic subse specif page. could execu code i	rability ading a ace to cl ious link quently fic web i A succes allow th te arbits in the co ed inter	d exploit by user of t ick a and access a nterface ssful exp ne attack rary scri- ntext of face or ve brow	he oloit er to pt the				
sg500x-24m	nn			D : CVE-						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remore condu script again based vulne insuff user-s web-baffect attack vulne persu interf malic subse	l interface Busines ged Switter an unaute attack act a crooking (XSS) st a user l interface rability ficient value supplied based interface act could rability ading a face to cl ious link equently	ss-site attack of the water. The didation input by terface of e. An d exploit by user of t ick a	and ald ated, web- of ythe of the athis the	N/A		H-CIS-S 041119	
CV Scoring Sca	le 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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
			could execu code affect acces based	allow the arbition the content of th	ve brow ation.	ter to pt the				
sg500x-24p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	based Small Mana allow remo condu script again based vulne insuff user- web-l affect attack vulne persu interf malic subse specif page. could execu code affect acces based	l interface Busines ged Swith an unaute attack act a crooting (XSS st a user l interface rability ficient value cased interface adding a face to clain ious link equently fic web i A succes allow the te arbite in the cole ed interface	ss-site c) attack cof the vece. The is due to alidation l input b terface of ee. An d exploit by user of t ick a access a nterface ssful exp ne attack cary scri ontext of face or ve brow ation.	and uld ated, web- of the this the coloit ser to pt the the	N/A		H-CIS-S 041119	
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	D	escription	& CVE II	D	Pate	ch	NCIIP	CID
			1271	8						
sg500x-48										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	Mana allow remote condustription again based vulne insuff users web-laffect attack vulne persuinterf malic subset specific page. could execut code affect acces based CVE I	Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718					H-CIS-S 041119	
sg500x-48mp	pp		A vulnerability in the web-							
Improper Neutralizati on of Input During Web Page Generation	16-10-2019	4.3	based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to				N/A		H-CIS-S 041119	
CV Scoring Sca (CVSS)	o-1	1-2	2-3	3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
('Cross-site Scripting')			condu scripti agains based vulner insuffi user-s web-b affecte attack vulner persua interfa malici subsect specifi page. A could a execut code in affecte access based	ct a cro ing (XSS it a user interface rability cient va upplied ased in ed device er could cability ading a ace to cl ous link quently ic web i A succes allow th te arbite in the co ed interface sensiti informa C: CVE-	ss-site s) attack of the v ce. The is due to alidation l input b terface o e. An d exploit by user of t ick a access a nterface rary scri ontext of face or ve brow ation.	veb- of of the this the ter to pt the				
sg500x-48p										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches 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				N/A		H-CIS-S 041119	
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface page. 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-2019-12718 Sg500xg-8f8t A vulnerability in the web-based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a specific web interface.	Weakness	Publish Date	cvss	D	escriptio	n & CVE II	D	Pato	h	NCIIP	C ID
sg500xg-8f8t A vulnerability in the webbased interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the webbased interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a				attack vulne persu interf malic subse specif page. could execu code i	ter could rability ading a ace to clious link quently fic web i allow the arbitrin the coed inters s sensiti	d exploit by user of t ick a and access a nterface ssful exp ne attack rary scri ontext of face or ve brow	he cloit eer to pt the				
A vulnerability in the web- based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and subsequently access a	sa500va-8f8t			CVE I	D : CVE-						
·	Improper Neutralizati on of Input During Web Page Generation ('Cross-site		4.3	based Small Mana allow remore condu script again based vulne insuff user-s web-baffect attack vulne persu interf malic subse	based interface of Cisco Small Business Smart and Managed Switches 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 device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and						

(CVSS)

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
Citrix			could execu code i affect access based	A succest allow the arbitroin the coed interest information of the coed in the	ne attack rary scri ntext of face or ve brow ation.	er to pt the				
netscaler_gat	teway									
Improper Authenticati on	21-10-2019	7.5	Citrix Contr Gatev 70.8, build build before attack mana access authe applia access forme NetSo	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway before 10.5 build 70.8, 11.x before 11.1 build 63.9, 12.0 before build 62.10, 12.1 before build 54.16, and 13.0 before build 41.28. An attacker with management-interface access can bypass authentication to obtain appliance administrative access. These products formerly used the NetScaler brand name. CVE ID: CVE-2019-					H-CIT-N 041119	
application_d	lelivery_contr	oller						Ī		
Improper Authenticati on	21-10-2019	7.5	Citrix Contr Gatev 70.8, build build	Applica oller (Al vay befo 11.x befo 63.9, 12 62.10, 1 54.16, a	tion Del DC) and re 10.5 l ore 11.1 .0 before 2.1 befo	ivery ouild e	N/A		H-CIT-A 041119	
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	D	escriptio	n & CVE I	D	Pate	h	NCIIP	CID
			mana acces authe applia acces forme NetSo	attacker with management-interface access can bypass authentication to obtain appliance administrative access. These products formerly used the NetScaler brand name. CVE ID: CVE-2019- 18225						
gateway										
Improper Authenticati on	21-10-2019	7.5	Citrix Contr Gatev 70.8, build build build befor attack mana acces authe applia acces forme NetSo	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway before 10.5 build 70.8, 11.x before 11.1 build 63.9, 12.0 before build 62.10, 12.1 before build 54.16, and 13.0 before build 41.28. An attacker with management-interface access can bypass authentication to obtain appliance administrative access. These products formerly used the NetScaler brand name.					H-CIT-0 041119	
comtechefda	ta									
h8_heights_re	emote_gatew	ay								
Improper Neutralizati on of Input During Web Page Generation	17-10-2019	3.5	Remo devic HTMI	ech H8 F ote Gatev es allow L'injection e (aka Sit	vay 2.5.2 XSS and on via th	l e Site	N/A		H-COM- 041119	_
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	Pul	blish Date	e CVSS	D	Description & CVE ID CVE ID : CVE-2019-				atch	NCIIP	PCID
('Cross-site Scripting')				CVE I 1766	_	2019-					
Dlink											
dir-412											
Improper Authenticati on	16-	10-2019	6.4	interfauther requipment of the clear via act=contour could attack	e are son faces with rements 12 A1-1 rs. An at the rout lear&log clear.pl be used traces. D: CVE- 2	hout on D-Li .14WW tacker c er's log f type=sy np, whic to erase	an file rsact h	N/A		H-DLI-I 041119	
dir-866l											
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-	10-2019	4.3	device Htmll the de gatew to con	k DIR-80 es allow Respons evice con vay inter nmon in D: CVE-	XSS via eMessag nmon face, lea jection.	ge in	N/A		H-DLI-I 041119	
eq-3											
homematic_c	ccu3										
Session Fixation	17-	10-2019	4.9	firmw sessic attack IDs ar victin logs it attack	eQ-3 HomeMatic CCU3 firmware 3.41.11 allows session fixation. An attacker can create session IDs and send them to the victim. After the victim logs in to the session, the attacker can use that session. The attacker			N/A		H-EQI 041119	
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE I	D	Pate	ch	NCIIP	CID
			after a easily systen	create S a valid so compro n. D: CVE-	ession a omise th	nd				
			_	HomeMa						
Improper Input Validation	17-10-2019	9	firmware version 3.41.11 allows Remote Code Execution in the ReGa.runScript method. An authenticated attacker can easily execute code and compromise the system.				N/A		H-EQH 041119	
			CVE I 1585	D : CVE- O	2019-					
ccu2										
Improper Control of Generation of Code ('Code Injection')	17-10-2019	9	A Remote Code Execution (RCE) issue in the addon CUx-Daemon 1.11a of the eQ-3 Homematic CCU- Firmware 2.35.16 until 2.45.6 allows remote authenticated attackers to execute system commands as root remotely via a simple HTTP request. CVE ID: CVE-2019- 14423				N/A		H-EQ0 041119	
Information Exposure	17-10-2019	4	A Local File Inclusion (LFI) issue in the addon CUx-Daemon 1.11a of the eQ-3 Homematic CCU-Firmware 2.35.16 until 2.45.6 allows remote authenticated attackers to read sensitive files via a simple HTTP Request.				N/A		H-EQ0 041119	
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	C ID
			CVE I 1442	D : CVE- 4	2019-					
hinet										
gpon										
Improper Input Validation	17-10-2019	7.5	handl discor firmw I0400 allow execu comm 3097 10.0. (CVSS N/UI:	An ?invalid command? handler issue was discovered in HiNet GPON firmware < 1040GWR190731. It allows an attacker to execute arbitrary command through port 3097. CVSS 3.0 Base score 10.0. CVSS vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:H/I:H/A:H). CVE ID: CVE-2019-				tvn.tw tw/ta TVN- 005, www. rg.tw 128- adb-	H-HIN-0 041119	
			1341		2019-					
Information Exposure	17-10-2019	5	on po GPON I0400 an att specif arbiti Base s vecto (CVSS N/UI:	A service which is hosted on port 3097 in HiNet GPON firmware < I040GWR190731 allows an attacker to execute a specific command to read arbitrary files. CVSS 3.0 Base score 9.3. CVSS vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:H/I:N/A:L). CVE ID: CVE-2019-				tvn.tw tw/ta TVN- 006, www. rg.tw 128- 4b1-	H-HIN-(041119	
Improper Authenticati on	17-10-2019	7.5	HiNet GPON firmware version < I040GWR190731 allows an attacker login to device without any authentication. CVE ID: CVE-2019-			ws	https://tcert.org.iwanvn/ 2019080 https://ttwcert.org/en/cp-23015-17	tw/ta TVN- 007, www. rg.tw	H-HIN-0 041119	
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	D	escriptio	n & CVE II	D	Pato	:h	NCIIP	C ID
			1506	4			2.html			
Information Exposure	17-10-2019	5	GPON 10400 an att specifi arbitr Base s vecto (CVSS N/UI:	on port 6998 in HiNet GPON firmware < I040GWR190731 allows an attacker to execute a specific command to read arbitrary files. CVSS 3.0 Base score 9.3. CVSS vector: (CVSS:3.0/AV:N/AC:L/PR: N/UI:N/S:C/C:H/I:N/A:L). CVE ID: CVE-2019- 15065				tvn.tw tw/ta TVN- 011, www. rg.tw 128- e90-	H-HIN-0 041119	
Improper Input Validation	17-10-2019	10	handl discor firmw I0400 allow execu comn 6998 10.0. (CVSS N/UI:	er issue vered in vare < GWR190 s an atta te arbitrand thr CVSS 3. CVSS vectors (CVSC)	was HiNet G 731. It cker to cary ough po 0 Base s ctor: :N/AC:L	PON rt core /PR:	https://cert.org. iwanvn/ 2019080 https://twcert.o /en/cp-1 3017-fd0 2.html	tw/ta TVN- 012, www. rg.tw 128-	H-HIN-0 041119	
Honeywell			1000							
ip-ak2										
Missing Authenticati on for Critical Function	25-10-2019	5	In IP-AK2 Access Control Panel Version 1.04.07 and prior, the integrated web server of the affected devices could allow remote attackers to obtain web configuration data, which can be accessed without authentication			N/A		H-HON- 041119		
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	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pate	:h	NCIIP	C ID
				3,32	the netw I D : CVE 25						
НР											
laserjet_ente	rpri	se_m653	3_j8a06a	l							
Improper Input Validation	16-	10-2019	7.5	Laser have appli may a execu code.	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-L 041119	
laserjet_man	aged	l_e6505	0_l3u55	a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.					H-HP-LA 041119	
laserjet_man	aged	l e6505	0 13u56a								
Improper Input Validation		10-2019		HP La Office Laser have appli may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-L 041119	
laserjet_man	aged	l_e6505	0_l3u57	7a							
Improper Input	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and			N/A		H-HP-LA 041119		
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
Validation			LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334		
laserjet_man	aged_e65060_	13u55a	E .		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1531
laserjet_man	aged_e65060_	13u56a	F		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1532
laserjet_man	aged_e65060_	13u57a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1533

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publi	ish Date	CVSS	D	escriptio	n & CVE I	D		Pato	h	NCIIF	PCID
laserjet_ente	rprise	_m750_	_d3l08a	ı								
Improper Input Validation	16-10	0-2019	7.5	Office Laser have applie may a execu- code.	aserJet, FeJet EnterJet Mana a solution cation si allow position of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A	A		H-HP-L 041119	
laserjet_ente	rprise	_m750_	_d3l09a									
Improper Input Validation	16-10	0-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check				N/A	Α		H-HP-L 041119	
laserjet_ente	rprise	_m750_	_d3l10a	1								
Improper Input Validation	16-10	0-2019	7.5	Office Laser have applie may a execu- code.	aserJet, FeJet EnterJet Mana a solution cation si allow position of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A	A		H-HP-L 041119	
laserjet_ente	rprise	_m751_	_t3u43a	1								
Improper Input Validation	16-10	0-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A	A		H-HP-L 041119	
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	D	escriptio	1 & CVE I	D		Pat	ch	NC	IIPC ID
			code.								
			CVE I	D : CVE-	2019-6	334					
laserjet_ente	erprise_m751_t	t3u44a	l								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	IserJet, For Enter Jet Mana a solution signification of a	rprise, a nged Pri n to che gnature tential rbitrary	nnd nters eck that	N/	A			-LASE- 19/1538
lacariat anto	erprise_m751_t	t3u64a	CVE ID : CVE-2019-6334								
iasei jet_eiitt	prise_iii/ 51_i	i3u04d	1	Y . =	Y 4 71 7						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/	A			-LASE- 19/1539
laserjet_mar	naged_e75245_	t3u43a	<u> </u>								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/	A			-LASE- 19/1540	
laserjet_mar	naged_e75245_	t3u44a	ła				l				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			ınd nters	N/A			H-HP-LASE- 041119/1541	
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_e75245_	t3u64a	l		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1542
laserjet_ente	rprise_m855_a	a2w77	a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1543
laserjet_ente	rprise_m855_a	a2w78	a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1544
laserjet_ente	rprise_m855_a	a2w79	a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
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	Pu	blish Date	CVSS	D	escriptio	n & CVE I	D		Pato	h	NCIII	PC ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				041119	9/1545
laserjet_ente	rpri	se_m85	5_d7p72	a								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu	serJet, Felet Enter Jet Mana solution singled by the serion of a s	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A	A		H-HP-L 041119	
laserjet_ente	rpri	se_m85	5_d7p73	a								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Enter Jet Mana a solution single grantion single grantion of a section	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A			H-HP-L 041119	
lacariat anta	rnri	sa flow	mfn m5			2019-0	334					
Improper Input Validation		10-2019		77_b5l46a HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A	A		H-HP-L 041119	
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	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
laserjet_ente	rprise_flow_m	fp_m5	77_b5l	47a						
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_ente	rprise_flow_m	fp_m5	77_b5l48a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check				N/A		H-HP-L. 041119	
laserjet_ente	rprise_flow_m	fp_m5	77_b5l	54a						
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	serJet, Polet Enter Jet Mana a solution cation signallow polution of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/A		H-HP-L. 041119	
laseriet ente	rprise_mfp_m	577 h5								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L. 041119	
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
			code.		
			CVE ID : CVE-2019-6334		
laserjet_ent	erprise_mfp_m	577_b5	5147a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1553
			CVE ID: CVE-2019-6334		
laserjet_ent	erprise_mfp_m	577_b5	5148a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1554
laserjet_ent	erprise_mfp_m	577_b5	il54a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1555
laserjet_mai	naged_flow_mfp	o_m577	7_b5l49a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1556
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	_m57	7_b5l50a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1557
laserjet_man	laged_mfp_m5'	 77_b5l	19a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1558
laserjet_man	aged_mfp_m5	77_b5l	50a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1559
laserjet_ente	rprise_flow_m	fp_m6	80_ca251a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pring In to che gnature tential Inbitrary	nters ck that			041119	/1560
laserjet_ente	rprise_flow_m	fp_m6	80_cz2	48a						
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu code.	serJet, Fet Ente Jet Mana a solution cation si allow po- tion of a	rprise, a aged Prin on to che gnature tential arbitrary	nd nters ck that	N/A		H-HP-L. 041119	
laseriet ente	rprise_flow_m	fn m6			2017-0	JJT				
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have applie may a execu	serJet, F Jet Ente Jet Mana a solutio cation si allow po tion of a	rprise, a nged Prin n to che gnature tential nrbitrary	nd nters ck that	N/A		H-HP-L. 041119	
				D : CVE-	2019-6	334				
laserjet_ente	rprise_flow_m	fp_m6								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119		
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	D	escription	n & CVE II	D		Pato	h	NCIIP	C ID
laserjet_ente	rprise_mfp_m	680_ca	251a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	serJet, Post Enter Jet Mana a solution cation signallow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/	'A		H-HP-L. 041119	
laserjet_ente	rprise_mfp_m	680_cz	248a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/	'A		H-HP-L. 041119	
laseriet ente	rprise_mfp_m	680 cz		D : CVE-							
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have a applie may a execu	serJet, P Jet Enter Jet Mana a solutio cation sig illow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/	'A		H-HP-L. 041119	_
laserjet_ente	rprise_mfp_m	680_cz	250a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/	'A		H-HP-L. 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Da	ite CVS	D	escription	n & CVE I	D	P	atch	NCIIP	PC ID	
			code.	D : CVE-	2019-6	334					
laserjet_man	aged_flow	mfp_m6	30_l3u4	7a							
Improper Input Validation	16-10-202	19 7.5	Office Laser have appli- may a execu- code.	eserJet, Fe Jet Enter Jet Mana a solution signation of a left.	rprise, a nged Pri n to che gnature tential rbitrary	and nters eck that	N/A		H-HP-LASI 041119/1		
laserjet_man	aged_flow	mfp_m6	30_l3u4	8a							
Improper Input Validation	16-10-202	19 7.5	Office Laser have appli- may a execu- code.	eserJet, Felet Enter Jet Mana a solution cation of a licential Enter Service Enter Service Enter Service Enter Service Enter Service Enter	rprise, a nged Pri n to che gnature tential rbitrary	and nters eck that	N/A		H-HP-L 041119		
laserjet_man	aged_mfp_	m680_l3	u47a								
Improper Input Validation	16-10-202	19 7.5	Office Laser have appli- may a execu- code.	eserJet, Felet Enter Jet Mana a solution signification of a section of	rprise, a nged Pri n to che gnature tential rbitrary	and nters eck that	N/A		H-HP-L 041119		
laserjet_man	aged_mfp_	m680_l3	u48a	48 a							
Improper Input Validation	16-10-202	7.5	Office Laser	aserJet, F eJet Ente ·Jet Mana a solutio	rprise, a nged Pri	nd nters	N/A		H-HP-L 041119		
CV Scoring Sca	ole 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_ente	erprise_flow_m	fp_m6	81_j8a10a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1572
laserjet_ente	erprise_flow_m	fp_m6	81_j8a11a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1573
laserjet_ente	erprise_flow_m	fp_m6	81_j8a12a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1574
laserjet_ente	rprise_flow_m	fp_m6	B1_j8a13a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	CID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pring In to che gnature tential Inbitrary	nters ck that			041119	/1575
laserjet_ente	rprise_flow_m	fp_m6	82_j8a	16a						
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu code.	serJet, Feder Enter Jet Mana a solution single grant on single grant of a section o	rprise, a aged Prin on to che gnature tential orbitrary	nd nters ck that	N/A		H-HP-L. 041119	
laseriet ente	rprise_flow_m	fn m6			2019-0	334				
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have applie may a execu	serJet, F Jet Ente Jet Mana a solutio cation si allow po tion of a	rprise, a nged Prin n to che gnature tential nrbitrary	nd nters ck that	N/A		H-HP-L. 041119	
				D : CVE-	2019-6	334				
laserjet_ente	rprise_mfp_m	681_j8			¥44. ¥					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
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	D	escription	n & CVE I	D	Pat	ch	NCIIP	C ID
laserjet_ente	rprise_mfp_m	681_j8	a11a_							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	serJet, P Jet Ente Jet Mana a solutio cation sig illow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_ente	rprise_mfp_m	681_j8	a12a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-LASE- 041119/1580	
laserjet_ente	rprise_mfp_m	681_j8	a13a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L. 041119	
lacariat anta	rnrica mfn m	602 (0		D.CVE-	2019-0	334				
iaserjet_ente	rprise_mfp_m	002_J8		serlet D	ageWid	e				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L. 041119	
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				
			code.						
			CVE ID: CVE-2019-6334						
laserjet_ent	erprise_mfp_m	682_j8	a17a						
Improper Input Validation	16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1583				
			CVE ID : CVE-2019-6334						
laserjet_mai	naged_flow_mfp	50_l3u66a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1584				
laserjet_mai	 naged_flow_mfj	p_e675	50_l3u67a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1585				
laserjet_mai	naged_flow_mfp	o_e675	50_l3u69a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1586				
CV Scoring Sc (CVSS)	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		
			application signature that may allow potential execution of arbitrary code.				
			CVE ID : CVE-2019-6334				
laserjet_man	aged_flow_mfp	e675_e	50_l3u70a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1587		
laserjet_man	aged_flow_mfp	e675	60_l3u66a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1588		
laserjet_ente	rprises_cp552	5_ce70	 9a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1589		
laserjet_man	aged_e55040d	lw_3gx	98a		• •		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-		
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	D	Description & CVE ID				ch	NCIIP	C ID
Input Validation			Laser have a applic may a execu code.	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pring on to che gnature tential arbitrary	nters ock that			041119	/1590
laserjet_man	aged_flow_mfj	p_e778	22_x3	a77a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_e77	/825_z8	3 z00a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L. 041119	
				D : CVE-	2019-6	334				
laserjet_man	aged_mfp_e77	825_z8								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119		
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
laserjet_man	aged_mfp_e77	825_z8	Bz04a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1594
laserjet_man	aged_mfp_e77	830_x3	Ba78a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1595
lacariat man	aged_mfp_e77	930 v3			
laserjet_man	aged_mip_e//	83U_X3		l	1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1596
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e77	830_x3	3a84a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1597
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	NCIIPC ID
			code.		
			CVE ID : CVE-2019-6334		
laserjet_man	naged_flow_mfp	o_e876	40_x3a89a		
Improper Input Validation	16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1598
			CVE ID: CVE-2019-6334		
laserjet_mar	naged_flow_mfp	40_x3a90a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1599
laserjet_man	naged_flow_mfp	e876	40_x3a92a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1600
laserjet_man	naged_flow_mfp	o_e876	40_x3a93a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1601
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	p_e876	40_z8z12a		1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1602
laserjet_man	laged_flow_mfp	40_z8z13a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1603
laserjet_man	aged_flow_mfp	p_e876	40_z8z14a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1604
laserjet_man	 aged_flow_mfj	o_e876			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9					

Weakness	Pu	blish Date	cvss	D	escriptio	n & CVE I	D		Patcl	h	NCIIP	CID
Input Validation				Laser have applie may a execu	CVE ID : CVE-2019-6334						041119	/1605
laserjet_man	aged	d_flow_n	1fp_e876	40_z8	z16a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-LASE- 041119/1606	
laseriet man	aged	l flow n	ıfn e876			2017 0						
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.						H-HP-L 041119	
laserjet_man	aged	l_flow_n	1fp_e876	550_x3	a86a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A			H-HP-L 041119		
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	D	escription	n & CVE I	D	Pat	ch	NCIIP	C ID
laserjet_man	aged_flow_mf	p_e876	50_x3	a87a						
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a nged Prin n to che gnature tential nrbitrary	nd nters ck that	N/A		H-HP-L. 041119	
laserjet_man	aged_flow_mf	p_e876	50_x3	a89a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_flow_mf	p_e876	50_x3a	a90a						
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L. 041119	
lacariat man	agad flavy mfr	0076			2019-0	JJ4				
iaserjet_man	aged_flow_mf	μ_eσ/6			logo MI: 1	•				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L 041119	
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 Dat	te CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
			code.							
			CVE I	D : CVE-	2019-6	334				
laserjet_man	aged_flow_	mfp_e876	50_x3	a93a						
Improper Input Validation	16-10-201	9 7.5	Office Laser have applie may a execu- code.	serJet, F Jet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L. 041119	
			CVE ID : CVE-2019-6334							
laserjet_managed_flow_mfp_e87650_z8z12a										
Improper Input Validation	16-10-201	9 7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		H-HP-L. 041119	_
laserjet_man	agged flow	mfn 0876		D : CVE-	2019-0	334				
laserjet_man	lageu_IIow_	шир_ео / о			Y 4 71 1					
Improper Input Validation	16-10-201	9 7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_flow_	mfp_e876	50_z8z	z14a						
Improper Input Validation	16-10-201	9 7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		N/A		H-HP-LASE- 041119/1616			
CV Scoring Sca (CVSS)	ale 0-1	e 0-1 1-2 2-3 3-4 4-5 5-6		5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			application signature that may allow potential execution of arbitrary code.			
			CVE ID : CVE-2019-6334			
laserjet_man	aged_flow_mfp	o_e876	50_z8z15a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1617	
laserjet_man	aged_flow_mfp	50_z8z16a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1618	
laserjet_man	laged_flow_mfp	o_e876	50_z8z17a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1619	
laserjet_man	 aged_flow_mfp	o_e876	60_x3a86a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-	
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	·				P	atch	NCIIP	CID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solutio cation si allow po tion of a	aged Pring In to che gnature tential Inbitrary	nters ock that			041119	/1620
laserjet_man	aged_flow_mfj	o_e876	60_x3	a87a						
Improper Input Validation	16-10-2019	7.5	may allow potential execution of arbitrary code.				N/A		H-HP-L. 041119	
lagariet man	agad flavy mfr	2 0076		D : CVE-	2019-6	334				
laserjet_man	aged_flow_mfj)_e876			DogoWid					
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L. 041119	
			CVE I	D : CVE-	2019-6	334				
laserjet_man	aged_flow_mfj	o_e876	60_x3	a90a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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
laserjet_man	aged_flow_mfp	e876	60_x3a92a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1624
laserjet_man	aged_flow_mfp	e876	60_x3a93a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1625
lacariat man	aged_flow_mfj	2 0876			
laser jet_illali	lageu_now_mij	J_eo70			I
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1626
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	_e876	60_z8z13a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1627
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	Publi	sh Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
				code.							
				CVE I	D : CVE-	2019-6	334				
laserjet_man	aged_f	flow_mf	p_e876	60_z8z	z14a						
Improper Input Validation	16-10)-2019	7.5	Office Laser have a applie may a execu code.	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L. 041119	
1		G 0	05.6			-2019-0	334				
laserjet_man	aged_1	llow_mf	p_e876	HP LaserJet, PageWide,							
Improper Input Validation	16-10)-2019	7.5	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check				N/A		H-HP-L. 041119	_
laserjet_man	aged f	flow mf	n e876								
laser jet_iliali	ageu_i	iiow_iiii	p_eo/0) \\A7: J	_				
Improper Input Validation	16-10)-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_f	flow_mf	p_e876	660_z8z17a							
Improper Input Validation	16-10)-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check				N/A		H-HP-L. 041119	
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish	Date	CVSS	D	escriptio	n & CVE I	D	Pato	ch	NCIIP	C ID
				may a	cation signallow postion of a	tential					
				CVE I	D : CVE-	2019-6	334				
laserjet_man	aged_mf	p_e87	7640_x	3a86a							
Improper Input Validation	16-10-2	019	7.5					N/A		H-HP-LA 041119	
laserjet_man	aged_mf	p_e87	7640_x								
Improper Input Validation	16-10-2	2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-LA 041119	
laserjet_man	aged_mf	p_e87	7640_x	3a89a							
Improper Input Validation	16-10-2	2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-LA 041119	
laserjet_man	aged_mf	p_e87	7640_x	x3a90a							
Improper	16-10-2	2019	7.5	HP LaserJet, PageWide,			N/A		H-HP-L	ASE-	
CV Scoring Sca (CVSS)	le ₀ .	1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	Pa	atch	NCIIF	C ID
Input Validation				Laser have applie may a execu- code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1635
laserjet_man	aged	l mfp et	87640 x		2.0.2						
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	aserJet, Felet Ente Jet Mana a solution cation si allow po ation of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l_mfp_e	87640_x	3a93a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Enter Jet Mana a solution single allow position of a court of the court	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l mfn e	87640 z		D T G V E	2017 0					
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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	D	escription	n & CVE II	D	F	atch	NCIIP	C ID
laserjet_man	aged_mfp_e87	640_z8	3 z 13a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a nged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L 041119	
laserjet_man	aged_mfp_e87	640_z8	3 z14 a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
laserjet_man	aged_mfp_e87	'640_z8	3 z15 a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	serJet, Pet Ente Jet Mana a solutio cation signallow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L 041119	
laceriet man	aged_mfp_e87	640 7 8		D.CVL	2017 0	JJ 1				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L 041119	
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	Pub	lish Date	CVSS	D	escriptio	n & CVE I	D	Pate	:h	NCIIP	C ID
				code.							
				CVE I	D : CVE-	2019-6	334				
laserjet_man	aged_	_mfp_e8	37640_z8	3 z 17a							
Improper Input Validation	16-1	0-2019	7.5	Office Laser have appli- may a execu- code.		rprise, anged Pri on to che gnature tential orbitrary	nnd nters eck that	N/A		H-HP-L. 041119	_
					D : CVE-	2019-6	334				
laserjet_man	aged_	_mfp_e8	37650_x3	3a86a							
Improper Input Validation	16-1	0-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		H-HP-L. 041119	
_					D : CVE-	2019-6	334				
laserjet_man	aged_	_mfp_e8	37650_x3	3a87a							
Improper Input Validation	16-1	0-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged_	_mfp_e8	37650_x3	3a89a							
Improper Input Validation	16-1	0-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			N/A		H-HP-L. 041119		
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e87	650_x3	3a90a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1647
laserjet_man	erjet_managed_mfp_e87650_x3a92a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1648
laserjet_man	aged_mfp_e87	650_x3	 		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1649
laserjet_man	aged_mfp_e87	650_z8	Bz12a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	Pa	tch	NCIIP	C ID
Input Validation				Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1650
laserjet_man	aged	l_mfp_e8	37650_z	8 z13 a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu code.	serJet, Forter Jet Mana a solution single a solution single a solution of a solution o	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l mfn e8	37650 z		2.0.2						
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l mfn es	37650 7		D. CVE	2017 0	331				
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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
laserjet_man	aged_mfp_e87	650_z8	Bz16a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1654
laserjet_man	aged_mfp_e87	650_z8	Bz17a	1	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1655
lagarist man		((0)			
laserjet_man	aged_mfp_e87	66U_X			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1656
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e87	660_x3	3a8 7 a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1657
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	Pub	lish Date	cvss	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	CID
				code.							
				CVE	D : CVE-	2019-6	334				
laserjet_mar	aged	_mfp_e	87660_x	3a89a							
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu code.		rprise, anged Pri on to che gnature tential orbitrary	nnd nters eck that	N/A		H-HP-LASE- 041119/165	
1		C	07660		D : CVE-	2019-0	334				
laserjet_mar	aged	_mtp_ea	6766U_X	1			1		T		
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		H-HP-L. 041119	
					D : CVE-	2019-6	334				
laserjet_man	aged	_mfp_e	87660_x	3a92a							
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			nnd nters eck that	N/A		H-HP-L 041119	
laserjet_mar	aged	_mfp_e	87660_x	3a93a							
Improper Input Validation	16-2	16-10-2019 HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		OfficeJet Enterprise, and LaserJet Managed Printers				N/A		H-HP-L 041119	
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e87	660_z8	Bz12a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1662
laserjet_man	erjet_managed_mfp_e87660_z8z13a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1663
laserjet_man	aged_mfp_e87	660_z8	 		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1664
laserjet_man	aged_mfp_e87	660_z8	Bz15a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	P	atch	NCIIF	PC ID
Input Validation				Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119)/1665
laserjet_man	aged	_mfp_e8	37660_z	8 z 16a							
Improper Input Validation	16-2	10-2019	7.5	Office Laser have applie may a execu code.	serJet, Forter Jet Mana a solution single allow position of a cut of the cut	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	_mfp_e8	37660_z	8 z17 a							
Improper Input Validation		10-2019	7.5	HP La Office Laser have applie may a execu	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nd nters eck that	N/A		H-HP-L 041119	
					D : CVE	-2019-6	334				
Improper Input Validation	16-2	se_ 500 _r	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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
laserjet_ente	erprise_500_m	551_cf()82a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1669
laserjet_ente	erprise_500_m	551_cf()83a	l	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1670
laserjet_ente	erprise_500_m	fp_m57	/5_cd644a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1671
			CVE ID : CVE-2019-6334		
laserjet_ente	erprise_500_mf	fp_m57	75_cd645a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1672
CV Scoring Sca (CVSS)	ole 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	D	escriptio	n & CVE I	D		Pato	:h	NCII	PC ID		
				code.										
				CVE	D : CVE	-2019-6	334							
laserjet_ente	rpri	se_500_	mfp_m5	75_cd6	46a									
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a	aserJet, I eJet Ente Jet Mana a solutio cation si allow po ation of a	erprise, a aged Pri on to che gnature tential	nters eck that	N/A			H-HP-LASE- 041119/167			
				CVE	D : CVE	-2019-6	334							
laserjet_enterprise_flow_mfp_m575_cd644a														
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A			N/A H-HP-LAS 041119/1				
laserjet_ente	rpri	se_flow_	mfp_m5	75_cd6	645a									
Improper Input Validation		10-2019		HP La Office Laser have appli may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		N/A		N/A		∠ASE- 9/1675
laserjet_ente	rpri	se_flow_	mfp_m5	75_cd6	646a									
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		N/A		H-HP-LASE- 041119/1676						
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.						
			CVE ID : CVE-2019-6334						
laserjet_man	aged_500_mfp	_m575	_l3u4 5 a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1677				
laserjet_managed_500_mfp_m575_l3u46a									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1678				
laserjet_man	 aged_flow_mfp		5_l3u45a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1679				
laserjet_man	 aged_flow_mfp		 5_l3u46a						
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-				
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	P	atch	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1680
laserjet_ente	rpri	se_500_	mfp_m5	25f_cf1	16a						
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Felet Enter Jet Mana solution singled by the control of a cont	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l_mfp_m	725_cf0	68a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	aserJet, Fet Enter Jet Mana a solution single allow position of a section of a sect	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l mfp m	725 cf0								
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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	D	escription	n & CVE II	D	Pa	tch	NCIIP	C ID
laserjet_man	aged_mfp_m7	25_l3u	63a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-L. 041119	
laserjet_man	aged_mfp_m7	25_l3u	64a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			and nters eck that N/A			H-HP-L. 041119	
laserjet_man	aged_mfp_e72	425_5	cm68a							
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have a applie may a execu	serJet, Pet Ente Jet Mana a solutio cation signallow pot tion of a	rprise, a aged Prin on to che gnature tential arbitrary	nd nters ock that	N/A		H-HP-L. 041119	
		40==		D : CVE-	2019-6	334				
laserjet_man	aged_mfp_e72	425_5								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L. 041119		
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	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pate	:h	NCIIP	C ID
				code.							
				CVE	D : CVE-	2019-6	334				
laserjet_mar	aged	l_mfp_e	72425_5	cm70a	l						
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a	aserJet, FeJet Ente Jet Mana a solution cation si allow po ation of a	rprise, and aged Price of the contraction of the co	nters eck that	N/A		H-HP-L. 041119	_
				CVE	D : CVE	2019-6	334				
laserjet_mar	aged	l_mfp_e	72425_5	cm71a	l						
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L. 041119	_	
					D : CVE-	2019-6	334				
laserjet_mar	aged	l_mfp_e	72425_5	cm72a	l						
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119	
laserjet_mar	naged	l_mfp_e	72425_5	rc89a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		N/A		H-HP-LASE- 041119/1691			
CV Scoring Sca (CVSS)	- I II-I I I-/ I /-3 I 3-Δ I Δ-5 I 5-h		5-6	6-7	7-8	8-9	9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
			application signature that may allow potential execution of arbitrary code.						
			CVE ID : CVE-2019-6334						
laserjet_man	aged_mfp_e72	425_51	rc90a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1692				
laserjet_managed_mfp_e72430_5cm68a									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1693				
laserjet_man	laged_mfp_e72	430_5	cm69a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1694				
laserjet_man	laged_mfp_e72	430_5	cm70a						
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-				
CV Scoring Sca (CVSS)	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	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	Pat	tch	NCIIF	C ID
Input Validation				Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1695
laserjet_man	aged	l_mfp_e7	72430_5	cm71a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Forter Jet Mana a solution single allow position of a court of the court of	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	anad	l mfn o'	72430 5			2019-0	334				
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l_mfp_e7	72430_5	rc89a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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
laserjet_man	aged_mfp_e72	430_51	rc90a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1699
laserjet_man	aged_flow_mfp	e725_e	25_x3a59a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1700
lacariat man	aged_flow_mfj	1 0725			
laser jet_illali	lageu_now_mij)_e/23			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1701
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	e725	25_x3a62a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1702
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	NCIIPC ID					
			code.							
			CVE ID : CVE-2019-6334							
laserjet_mar	naged_flow_mfp	o_e725	25_x3a63a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1703					
1	1.0	505	CVE ID : CVE-2019-6334							
laserjet_mar	laserjet_managed_flow_mfp_e72525_x3a65a									
Improper Input Validation	16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1704					
			CVE ID : CVE-2019-6334							
laserjet_mar	naged_flow_mfp	o_e725	25_x3a66a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1705					
laserjet_mar	naged_flow_mfp	e725	25_z8z010a		1					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	H-HP-LASE- 041119/1706						
CV Scoring Sco (CVSS)	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				
			application signature that may allow potential execution of arbitrary code.						
			CVE ID : CVE-2019-6334						
laserjet_man	aged_flow_mfj	o_e725	25_z8z011a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1707				
laserjet_managed_flow_mfp_e72525_z8z06a									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1708				
laserjet_man	laged_flow_mfj	p_e725	25_z8z07a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1709				
laserjet_man	 aged_flow_mfj	p_e725							
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-				
CV Scoring Sca (CVSS)	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	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pato	ch	NCIIP	C ID
Input Validation				Laser have applie may a execu code.	Jet Mana a solutic cation si allow po ation of a	rprise, a aged Pri on to che gnature tential arbitrary	nters ock that			041119	/1710
laserjet_man	aged	l_flow_m	fp_e725	25_z8	z09a						
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po ation of a	PageWid rprise, a aged Pri on to che gnature tential arbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_man	aged	l_flow_m	fp_e725	30_x3	a59a						
Improper Input Validation		10-2019	7.5	HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L. 041119	
laserjet_man	aged	l flow m	fn e725								
Improper Input Validation		10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119		
CV Scoring Sca (CVSS)	le	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
laserjet_man	aged_flow_mfp	e725	30_x3a62a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1714
laserjet_man	aged_flow_mfp	e725_e	30_x3a63a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1715
lagarist man		725			
laserjet_man	aged_flow_mfp	o_e725			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1716
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	e725	30_x3a66a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1717
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	Pub	lish Date	cvss	D	escriptio	a CVE I	D	Pate	ch	NCIIP	C ID
				code.							
				CVE I	D : CVE	2019-6	334				
laserjet_mar	aged	_flow_n	ıfp_e725	30_z8	z010a						
Improper Input 16-10-2019 Validation		7.5	Office Laser have appli- may a execu- code.		rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L. 041119		
					ID : CVE-	2019-6	334				
laserjet_managed_flow_mfp_e72530_z8z011a											
Improper Input Validation	16-1	0-2019	7.5	Office Laser have appli- may a execu- code.	aserJet, FeJet EnterJet Mana a solution cation si allow po ation of a	rprise, a nged Pri on to che gnature tential orbitrary	nnd nters eck that	N/A		H-HP-L. 041119	
lacariat man	nagad	flory n	fn 0725			2019-0	334				
laserjet_mar	iagea_	_IIOW_N	11p_e/25								
Improper Input Validation	16-1	.0-2019	7.5	Office Laser have appli- may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				H-HP-L. 041119		
laserjet_mar	aged	_flow_n	ıfp_e725	30_z8	z07a						
Improper Input Validation	16-1	.0-2019	7.5	Office Laser	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			H-HP-L. 041119			
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfj	o_e725	30_z8z08a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1722
laserjet_man	laged_flow_mfj	p_e725	30_z8z09a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1723
laserjet_man	aged_flow_mfj	p_e725	35_x3a59a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1724
laserjet_man	 aged_flow_mfj	o_e725			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pu	blish Date	e CVSS	D	escriptio	n & CVE I	D		Pato	:h	NCIII	PC ID
Input Validation				Laser have applie may a execu- code.	CVE ID : CVE-2019-6334						041119)/1725
laserjet_man	aged	d_flow_n	nfp_e725	535_x3	a62a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Enter Jet Mana solution singled allow position of a certain single and the cert	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A	Α		H-HP-L 041119	
laserjet_man	aged	l flow n	nfn e725									
Improper Input Validation		10-2019		HP La Office Laser have applie may a	IP LaserJet, PageWide, OfficeJet Enterprise, and aserJet Managed Printers ave a solution to check pplication signature that hay allow potential xecution of arbitrary			H-HP-L 041119				
laserjet_man	aged	l flow n	1fp e725									
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A	A		H-HP-L 041119	
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	D	escription	n & CVE I	D	Pa	tch	NCIIP	C ID
laserjet_man	aged_flow_mf	p_e725	35_x3	a66a						
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a nged Prin n to che gnature tential nrbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_man	aged_flow_mf	p_e725	35_z8z	z010a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	t_managed_flow_mfp_e72535_z8z011a									
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	serJet, Pet Ente Jet Mana a solution cation signallow poor tion of a	rprise, a aged Prin on to che gnature tential arbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laseriet man	aged_flow_mf	n e725								
Improper Input Validation	16-10-2019	7.5	35_z8z06a HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L. 041119	
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	Publ	ish Date	CVSS	D	escriptio	a CVE I	D	Pate	ch	NCIIP	C ID
				code.							
				CVE	ID : CVE-	2019-6	334				
laserjet_mar	aged_	flow_m	fp_e725	35_z8	z07a						
Improper Input 16-10-2019 Validation		0-2019	7.5	Office Laser have appli may a	aserJet, FeJet Ente Jet Mana a solution cation si allow po Ition of a	rprise, and aged Price of the contraction of the co	nters eck that	N/A		H-HP-L. 041119	_
					ID : CVE-	2019-6	334				
laserjet_managed_flow_mfp_e72535_z8z08a											
Improper Input Validation	16-1	0-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				H-HP-L. 041119	_	
lacariat mar	agod	flow m	fn 0725			2017 0	7334				
laserjet_mai	iageu_	110W_III	пр_е/25			Y 4 71 1	ı				
Improper Input Validation	16-1	0-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				H-HP-L. 041119		
laserjet_mar	aged_	mfp_e7	72525_x3	3a59a							
Improper Input Validation	16-1	0-2019	7.5	Office Laser	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			H-HP-L. 041119			
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e72	525_x3	Ba60a		1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1737
laserjet_man	laged_mfp_e72	525_x3	Ba62a		
Improper Input Validation	t 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1738
laserjet_man	laged_mfp_e72	525_ x3	Ba63a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1739
laserjet_man	 aged_mfp_e72	525_x3	<u> </u> 		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	Pa	itch	NCIIF	C ID
Input Validation				Laser have applie may a execu	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					041119	/1740
laserjet_man	aged	l mfn e'	72525 x		D. CVL	2017 0					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	userJet, Felet Enter Jet Mana a solution cation singles allow pontion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	_
laserjet_man	aged	l mfp e'	72525 z								
Improper Input Validation		10-2019		HP La Office Laser have applie may a	P LaserJet, PageWide, fficeJet Enterprise, and aserJet Managed Printers ave a solution to check oplication signature that ay allow potential kecution of arbitrary			H-HP-L 041119			
laserjet_man	aged	l mfn e'	72525 zi								
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L 041119	
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	D	escription	n & CVE II	D	P	atch	NCIIF	PCID
laserjet_man	aged_mfp_e72	2525_z8	3z06a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/A		H-HP-L 041119	
laserjet_man	aged_mfp_e72	2525_z8	3z07a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
laserjet_man	aged_mfp_e72	2525_z8	3 z 08a							
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have a applie may a execu	serJet, Pet Ente Jet Mana a solution cation signallow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/A		H-HP-L 041119	
lacoriot man	agod mfn o72) E 2 E 7 C		D. CVL	2017 0	JJ T				
iaserjet_iiiali	aged_mfp_e72	4343_Z0		serlet D	200Mid	Δ				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L 041119		
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	
			code.			
			CVE ID: CVE-2019-6334			
laserjet_ma	naged_mfp_e72	530_x3	Ba59a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1748	
			CVE ID : CVE-2019-6334			
laserjet_ma	naged_mfp_e72	530_x3	3a60a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1749	
laserjet_ma	naged_mfp_e72	530_x3	3a62a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1750	
laserjet_ma	naged_mfp_e72	530_x3	Ba63a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1751	
CV Scoring Sc (CVSS)	rale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e72	530_x3	Ba65a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1752
laserjet_man	aged_mfp_e72	530_x3	Ba66a		
Improper Input Validation	input 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1753
laserjet_man	aged_mfp_e72	530_z8	 		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1754
laserjet_man	aged_mfp_e72	530_z8	3z011a		•
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	C ID
Input Validation				Laser have applie may a execu- code.	CVE ID : CVE-2019-6334					041119	/1755
laserjet_man	aged	l_mfp_e	72530_z	8z06a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Enter Jet Mana a solution single grant on the section of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
lacariat man	2000	l flow n	1fn 0778			2017-0	.				
Improper Input Validation		10-2019		HP La Office Laser have applie may a				H-HP-L 041119			
laserjet_man	aged	l_flow_n	nfp_e778	322_x3	a83a						
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L 041119	
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	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
laserjet_man	aged_mfp_e77	/825_x3	3a78a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_e77	428_5	rc91a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
laserjet_man	aged_flow_mf	p_e778	22_z8z	z01a						
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	serJet, Polet Enter Jet Mana a solution signallow poletion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L 041119	
lacariat man	aged_flow_mf	n 0779			2017 0	JJ 1				
laser jet_illali	ageu_now_nn	P_6770	1		ageWid	P.				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L. 041119	
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 II	0	Pato	h	NCIIF	PC ID	
			code.						
			CVE ID : CVE-2019-6	334					
laserjet_mar	naged_flow_mfp	o_e778	22_z8z0a						
Improper Input Validation	16-10-2019 7.5		HP LaserJet, PageWide OfficeJet Enterprise, a LaserJet Managed Prin have a solution to che application signature may allow potential execution of arbitrary code.	nd nters ck that	N/A		H-HP-L 041119	_	
			CVE ID: CVE-2019-6	334					
laserjet_mar	naged_flow_mfp	e778	25_x3a77a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide OfficeJet Enterprise, a LaserJet Managed Prin have a solution to che application signature may allow potential execution of arbitrary code. CVE ID: CVE-2019-6.	nd nters ck that	N/A		H-HP-LASE 041119/17		
laserjet_mai	 naged_flow_mfj	e675	60_l3u67a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide OfficeJet Enterprise, a LaserJet Managed Prinhave a solution to che application signature may allow potential execution of arbitrary code. CVE ID: CVE-2019-6	nd nters ck that	N/A		H-HP-LASE 041119/17		
laserjet_mar	naged_flow_mfp	o_e675	60_13u69a						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide OfficeJet Enterprise, a LaserJet Managed Prin have a solution to che	nd nters	N/A		H-HP-LASE- 041119/1766		
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.							
			CVE ID : CVE-2019-6334							
laserjet_man	aged_flow_mfj	p_e675	60_l3u70a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1767					
laserjet_managed_mfp_e67550_l3u66a										
Improper Input Validation	Improper 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1768					
laserjet_man	 aged_mfp_e67	550_l3	u67a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1769					
laserjet_man	aged_mfp_e67	550_l3	u69a							
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-					
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10					

Weakness	Pul	olish Date	CVSS	D	escriptio	n & CVE I	D	Pat	tch	NCIIF	C ID
Input Validation				Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1770
laserjet_man	aged	l_mfp_e6	5 7550_ l3								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu code.	serJet, Forter Jet Mana a solution single allow position of a court of the court of	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l mfn eð	5 7560 13		D. CVE	2017 0					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L 041119	
laserjet_man	aged	l mfp e	57560 l3		_						
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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	D	escription	n & CVE II	D		Patch		NCIIP	C ID
laserjet_man	aged_mfp_e67	560_1 3	u69a								
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have a applie may a execu code. CVE I	N/A			H-HP-L. 041119				
laserjet_man	aged_mfp_e67	560_l 3	u70a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-L 041119	
laserjet_ente	rprises_cp552	25_ce7()7a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	serJet, Post Enter Jet Mana solution signation of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A			H-HP-L. 041119	
laseriet ente	rprises_cp552	25 ce70)8a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A			H-HP-L. 041119	
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	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pate	:h	NCIIP	C ID
				code.							
				CVE	D : CVE	2019-6	334				
laserjet_mar	naged	l_mfp_e	77825_x	3a81a							
Improper Input Validation	16-10-2019 7.5			Office Laser have appli may a execu code.		rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	_
			5500E (D : CVE-	2019-6	334				
laserjet_managed_mfp_e77825_x3a84a											
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu code.	LaserJet, PageWide, FiceJet Enterprise, and SerJet Managed Printers We a solution to check plication signature that The properties of the				H-HP-L. 041119	_	
	L				D : CVE-	2019-6	334				
laserjet_mar	aged	l_flow_n	nfp_e876	40_x3	a86a						
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			N/A	N/A		ASE- /1780
laserjet_mar	naged	l_flow_n	nfp_e876	40_x3	a87a						
Improper Input Validation	16-	10-2019	7.5	Office Laser	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		N/A		H-HP-L. 041119		
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	4-5 5-6 6-7 7-8		7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID					
			application signature that may allow potential execution of arbitrary code.							
			CVE ID : CVE-2019-6334							
laserjet_man	naged_flow_mfj	p_e778	25_x3a80a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1782					
laserjet_managed_flow_mfp_e77825_x3a83a										
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1783					
laserjet_man	naged_flow_mfj	o_e778	25_z8z01a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1784					
laserjet_man	 naged_flow_mfj	o_e778								
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-					
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	ı	Patch		NCIIP	CID
Input Validation				OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334							041119	/1785
laserjet_man	aged	d_flow_n	1fp_e778	25_z8	z0a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A			H-HP-L. 041119	
laserjet_man	2000	l flow n	ıfn 0779			2017-0	.					
lasei jet_illali	aget	1_110W_11	пр_е//с	_) \ A7: J	_					
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a	serJet, F Jet Ente Jet Mana a solutio cation si allow po tion of a	rprise, a aged Pri on to che gnature tential	nters eck that	N/A			H-HP-L. 041119	
				CVE I	D : CVE	·2019-6	334					
laserjet_man	aged	l_flow_n	1fp_e778	30_x3	a80a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A			H-HP-L. 041119		
CV Scoring Sca (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	Description & CVE ID	Patch	NCIIPC ID
laserjet_man	aged_flow_mfp	e778	30_x3a83a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1789
laserjet_man	aged_flow_mfp	e778	30_z8z01a	1	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1790
lacariat man	aged_flow_mfj	2 0779			
laserjet_man	aged_now_mij)_e//8		l	1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1791
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e77	830_z8	3z04a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1792
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	NCIIPC ID					
			code.							
			CVE ID : CVE-2019-6334							
laserjet_mai	naged_flow_mfp	e575_e	40_3gy25a							
Improper Input Validation	16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1793					
			CVE ID: CVE-2019-6334							
laserjet_managed_flow_mfp_e57540_3gy26a										
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1794					
laserjet_mai	naged_mfp_e57	540_3	gy25a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1795					
laserjet_mai	naged_mfp_e57	540_3	gy26a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1796					
CV Scoring Sc (CVSS)	rale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e77	422_5	cm75a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1797
laserjet_man	laged_mfp_e77	422_5	cm76a		
Improper Input Validation	nput 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1798
laseriet man	aged_mfp_e77	422 50			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1799
laserjet_man	aged_mfp_e77	422_5	cm78a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	C ID
Input Validation				Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1800
laserjet_man	aged	l mfp e'	77422 5		D. GVE	2017 0					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	aserJet, Felet Ente Jet Mana a solution cation si allow po ation of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l_mfp_e	77422_5	rc92a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L 041119	
laserjet_man	agad	l mfn a'	77420 F		D : CVE	-2019-0	334				
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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	D	escription	n & CVE II	D		Patc	h	NCIIF	C ID
laserjet_man	aged_mfp_e77	428_5	cm76a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	CVE ID : CVE-2019-6334						H-HP-L 041119	
laserjet_man	aged_mfp_e77	428_5 1	rc92a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	may allow potential execution of arbitrary						H-HP-L 041119	
laserjet_man	aged_flow_mf	p_e778	30_z8z	z0a							
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have a applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A			H-HP-L 041119	
laseriet man	aged_mfp_e77	/822 v		DIGIE							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A			H-HP-L 041119		
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
			code.		
			CVE ID : CVE-2019-6334		
laserjet_man	naged_mfp_e77	822_x3	Ba81a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1808
			CVE ID: CVE-2019-6334		
laserjet_man	naged_mfp_e77	822_x3	3a84a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1809
laserjet_man	naged_mfp_e77	822_z8	Bz00a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1810
laserjet_man	naged_mfp_e77	3z02a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1811
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e77	822_z8	Bz04a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1812
laserjet_man	aged_mfp_e77	830_z8	Bz00a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1813
laserjet_man	laged_mfp_e77	830_z8	 		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1814
laserjet_man	aged_mfp_e77	422_5	cm79a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	CID
Input Validation				Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1815
laserjet_man	aged	l_mfp_e7	77428_5	cm77a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu code.	serJet, Fet Enter Jet Mana a solution single allow position of a certain single and a certain of a certain single and a certa	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
lacariat man	200	l mfn o'	77420 E			-2019-0	334				
laserjet_man	ageo	ı_mıp_e	/ /428_5			YA7: 1					
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L 041119	
				CVE I	D : CVE	2019-6	334				
laserjet_man	aged	l_mfp_e7	77428_5	cm79a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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
laserjet_man	aged_mfp_e72	530_z8	Bz07a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1819
laserjet_man	aged_mfp_e72	530_z8	Bz08a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1820
lacariat man	aged_mfp_e72	530 78			
laser jet_illali	lageu_iiip_e/2	330_Z0			I
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1821
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e72	535_x3	3a59a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1822
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			code.							
			CVE I	D : CVE	2019-6	334				
laserjet_man	aged_mfp_e7	2535_x3	3a60a							
Improper Input Validation	nput 16-10-2019 7.5				rprise, and prise, and prise and pri	nd nters eck that	N/A		H-HP-L. 041119	
locariet man	agad mfn a7	2525 ***	CVE ID : CVE-2019-6334							
iaserjet_man	aged_mfp_e7	2535_X	1	• -				1		
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	may allow potential execution of arbitrary			N/A		H-HP-L. 041119	
				D : CVE-	2019-6	334				
laserjet_man	aged_mfp_e7	2535_x3	3a63a							
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				H-HP-L. 041119		
laserjet_man	aged_mfp_e7	2535_x3	3a65a							
Improper Input Validation	16-10-2019	7.5	Office Laser	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check					H-HP-L. 041119	
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e72	535_x3	Ba66a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1827
laserjet_man	aged_mfp_e72	535_z8	Bz010a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1828
laseriet man	aged_mfp_e72	535 z8			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1829
laserjet_man	aged_mfp_e72	535_z8	3z06a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119)/1830
laserjet_man	aged	mfp e7	2535 z		D. GVE	2017 0					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged _.	_mfp_e7	/2535_z	8 z 08a							
Improper Input Validation		10-2019	7.5	HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L 041119	
laserjet_man	aged	mfp_e7	/2535_z	8z09a							
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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
laserjet_man	aged_flow_mfp	e825	40_az8z20a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1834
laserjet_man	aged_flow_mfp	_e825	40_x3a68a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1835
lacariat man	 aged_flow_mfj	0825			
laserjet_man	aged_now_mij)_e825		l	1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1836
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	o_e825	40_x3a71a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1837
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	NCIIPC ID
			code.		
			CVE ID : CVE-2019-6334		
laserjet_mai	naged_flow_mfp	o_e825	40_x3a72a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1838
			CVE ID : CVE-2019-6334		
laserjet_mai	naged_flow_mfp	v_mfp_e82540_x3a74a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1839
laserjet_mai	naged_flow_mfp	e825	40_x3a75a		
Improper Input Validation	have a solution to check application signature that may allow potential execution of arbitrary code.		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1840
laserjet_mai	naged_flow_mfp	o_e825	40_x3a79a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1841
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfj	p_e825	40_x3a82a		1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1842
laserjet_man	laged_flow_mfj	p_e825	40_z8z18a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1843
laserjet_man	laged_flow_mfj	p_e825	40_z8z19		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1844
laserjet_man	 aged_flow_mf	o_e825			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 0-1	6-7 7-8	8-9 9-10		

Weakness	Pu	blish Date	e CVSS	D	escriptio	n & CVE I	D	P	atch	NCIIF	C ID
Input Validation				Laser have applie may a execu- code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119)/1845
laserjet_man	aged	d_flow_n	nfp_e825	540_z8	10_z8z23a						
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Enter Jet Mana solution singled by the second of a sec	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	d flow n	nfp e825								
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L 041119	
laserjet_man	0000	l flow n	ofn 0021			2019-0	334				
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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
laserjet_man	aged_flow_mfp	e825	50_x3a69a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1849
laserjet_man	aged_flow_mfp	e825_e	50_x3a71a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1850
laceriet man	aged_flow_mfj	1 6825			
laser jet_illali	lageu_now_mij)_eoz3			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1851
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	_e825	50_x3a74a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1852
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	Pub	lish Date	cvss	D	escriptio	a CVE I	D	Pate	ch	NCIIP	C ID	
				code.								
				CVE	D : CVE	2019-6	334					
laserjet_mar	aged	_flow_n	1fp_e825	50_x3	a75a							
Improper Input Validation	16-2	10-2019	7.5	Office Laser have appli may a execu code.		rprise, a aged Pri on to che gnature tential orbitrary	and nters eck that	N/A		H-HP-LASE- 041119/185		
					CVE ID : CVE-2019-6334							
laserjet_mar	aged	_flow_n	1fp_e825	50_x3	a79a							
Improper Input Validation	16-2	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		H-HP-L. 041119	_	
			4 00 7		D : CVE-	2019-6	334					
laserjet_mar	aged	_flow_n	1fp_e825									
Improper Input Validation	16-2	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119		
laserjet_mar	aged	_flow_n	1fp_e825	50_z8	z18a							
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			N/A		H-HP-LASE- 041119/1856			
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	5-6	5-6 6-7 7-8		8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			application signature that may allow potential execution of arbitrary code.			
			CVE ID : CVE-2019-6334			
laserjet_man	aged_flow_mfp	o_e825	50_z8z19		1	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1857	
laserjet_man	laged_flow_mfp	p_e825	50_z8z22a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1858	
laserjet_man	aged_flow_mfp	e825	50_z8z23a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1859	
laserjet_man	 aged_flow_mfp	o_e825	60_az8z20a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-	
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	Pu	blish Date	CVSS	D	escriptio	n & CVE I	D		Patc	h	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				041119)/1860
laserjet_man	aged	d_flow_n	nfp_e825	60_x3	a68a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu	may allow potential execution of arbitrary			N/A			H-HP-L 041119	
lacariat man	2000	l flow n	nfn 0825			2017 0						
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A			H-HP-L 041119	
laserjet_man	aged	d_flow_n	nfp_e825	660_x3	a71a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A			H-HP-L 041119		
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	
laserjet_man	aged_flow_mfp	e825	60_x3a72a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1864	
laserjet_man	aged_flow_mfp	e825_e	60_x3a74a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1865	
lacariat man	 aged_flow_mfj	0825				
laserjet_man	aged_now_mij)_e825		l	<u> </u>	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1866	
			CVE ID : CVE-2019-6334			
laserjet_man	aged_flow_mfp	o_e825	60_x3a79a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1867	
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	NCIIPC ID		
			code.				
			CVE ID : CVE-2019-6334				
laserjet_man	naged_flow_mfp	o_e825	60_x3a82a				
Improper Input 16-10-2019 Validation		7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1868		
			CVE ID : CVE-2019-6334				
laserjet_man	naged_flow_mfp	o_e825	60_z8z18a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1869		
1	1.0	025	CVE ID : CVE-2019-6334				
laserjet_man	naged_flow_mfp)_e825					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1870		
laserjet_mar	naged_flow_mfp	e825_e	60_z8z22a		•		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check H-HP-LA 041119/				
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.			
			CVE ID : CVE-2019-6334			
laserjet_man	aged_flow_mfj	p_e825	60_z8z23a		1	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1872	
laserjet_man	laged_mfp_e82	540_az	28 z 20a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1873	
laserjet_man	laged_mfp_e82	540_x3	3a68a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1874	
laserjet_man	laged_mfp_e82	540_x3	Ba69a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-	
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	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1875
laserjet_man	aged	l_mfp_e8	32540_x	3a 71 a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-L 041119	
laserjet_man	aged	l_mfp_e8	32540_x								
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L 041119	
laserjet_man	agod	l mfn o	22540 v		D. CVE	2019-0	334				
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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
laserjet_man	aged_mfp_e82	540_x3	3a75a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1879
laserjet_man	aged_mfp_e82	540_x3	Ba79a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1880
lacariat man	aged_mfp_e82	540 v3			
laserjet_man	aged_mip_e82	54U_X3		T	I
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1881
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e82	540_z8	3z18a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1882
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	Puk	olish Date	CVSS	D	escriptio	n & CVE I	D		Pato	:h		NCIIP	CID
				code.									
				CVE	D : CVE	2019-6	334						
laserjet_mar	aged	l_mfp_e	82540_z8	3z19									
Improper Input Validation	16-:	10-2019	7.5	Office Laser have appli may a execu code.		rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A			H-HP-LASE- 041119/188		
_					CVE ID : CVE-2019-6334								
laserjet_mar	aged	l_mfp_e	32540_z8z22a										
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A				H-HP-LA 041119	
					D : CVE-	2019-6	334						
laserjet_man	aged	l_mfp_e	82540_z8	3z23a									
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A				H-HP-LA 041119		
laserjet_mar	aged	l_mfp_e	82550_a	z8z20a	ı								
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		N/A				H-HP-L <i>i</i> 041119			
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	5-6	6 6-7 7-8			8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			application signature that may allow potential execution of arbitrary code.			
			CVE ID : CVE-2019-6334			
laserjet_man	aged_mfp_e82	550_x3	Ba68a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1887	
laserjet_man	aged_mfp_e82	550_x3	Ba69a			
Improper Input Validation	t 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1888	
laserjet_man	aged_mfp_e82	550_x3	 Ba71a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1889	
laserjet_man	aged_mfp_e82	550_x3	3a72a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-	
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	D	escriptio	n & CVE I	D	Pa	tch	NCIIP	CID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pring on to che gnature tential arbitrary	nters ock that			041119	/1890
laserjet_man	aged_mfp_e82	550_x	3a74a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_e82	550_x3		_						
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary		N/A		H-HP-L. 041119		
				D : CVE-	2019-6	334				
laserjet_man	aged_mfp_e82	550_x3								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334		N/A		H-HP-L. 041119			
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
laserjet_man	aged_mfp_e82	550_x3	3a82a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1894
laserjet_man	aged_mfp_e82	550_z8	3z18a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1895
lacariat man	agad mfn a02	FF0 =0			
laserjet_man	aged_mfp_e82	55U_Zt			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1896
			CVE ID : CVE-2019-6334		
laserjet_man	aged_mfp_e82	550_z8	Bz22a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1897
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	Pub	lish Date	CVSS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID					
				code.												
				CVE	D : CVE	2019-6	334									
laserjet_man	aged	_mfp_e	82550_z8	3z23a												
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu code.						H-HP-LAS 041119/1						
	<u> </u>				CVE ID : CVE-2019-6334											
laserjet_man	aged	_mfp_e	82560_a	z8z20a	1											
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A H-HP-LA 041119/		_							
					D : CVE-	2019-6	334									
laserjet_man	aged	_mfp_e	82560_x	3a68a												
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-LA 041119						
laserjet_man	aged	_mfp_e	82560_x	3a69a												
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			OfficeJet Enterprise, and LaserJet Managed Printers		OfficeJet Enterprise, and LaserJet Managed Printers		7.5 OfficeJet Enterprise, and LaserJet Managed Printers		N/A		H-HP-LA 041119	
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.			
			CVE ID : CVE-2019-6334			
laserjet_man	aged_mfp_e82	560_x3	Ba71a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1902	
laserjet_man	aged_mfp_e82	560_x3	Ba72a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1903	
laserjet_man	aged_mfp_e82	560_x3	Ba74a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1904	
laserjet_man	laged_mfp_e82	560_x3	Ba75a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-	
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	Pu	blish Date	CVSS	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	CID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1905
laserjet_man	aged	l_mfp_e8	32560_x	3a79a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	may allow potential execution of arbitrary		N/A		H-HP-LASE- 041119/190		
laserjet_man	aged	l mfn e8	32560 x		D. CVE	2017 0					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.		N/A		H-HP-L 041119		
laserjet_man	aged	l mfn e8	32560 z								
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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
laserjet_man	aged_mfp_e82	560_z8	3z19		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1909
laserjet_man	aged_mfp_e82	560_z8	3z22a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1910
locariot man	agad mfn a02	E60 70			
laserjet_man	aged_mfp_e82	56U_Z		T	T
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1911
			CVE ID : CVE-2019-6334		
officejet_ente	erprise_flow_n	ıfp_x58	35_b5106a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-OFFI- 041119/1912
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	NCIIPC ID
			code.		
			CVE ID : CVE-2019-6334		
officejet_ent	erprise_flow_n	ıfp_x58	35_b5l07a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-OFFI- 041119/1913
			CVE ID : CVE-2019-6334		
officejet_ent	erprise_flow_n	ıfp_x58	35_l3u41a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-OFFI- 041119/1914
officejet_ent	erprise_mfp_x	585_b5	104a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-OFFI- 041119/1915
officejet_ent	erprise_mfp_x!	585_b5	105a		
Improper Input Validation	16-10-2019	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-OFFI- 041119/1916	
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.			
			CVE ID : CVE-2019-6334			
officejet_ente	erprise_mfp_x	585_l3ı	140a		1	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-OFFI- 041119/1917	
officejet_mar	naged_flow_mf	p_x585	5_b5l06a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-OFFI- 041119/1918	
officeiet mar	 naged_flow_mf	p x585				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-OFFI- 041119/1919	
officejet_mar	naged_flow_mf	p_x585	_l3u41a		•	
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-OFFI-	
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 Da	te CVS	S C	escriptio	n & CVE I	D	Pat	tch	NCIIP	CID
Input Validation			Laser have appli may a execu		aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1920
				ID : CVE	-2019-6	334				
officejet_mar	naged_mfp_	x585_b	104a							
Improper Input Validation	16-10-201	.9 7.5	Office Laser have appli may execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.		N/A		H-HP-0 041119		
officejet_mar	aged mfn	v585 h		ID . CVE	2017-0	133 1				
onicejet_mai	lageu_lilip_	_XJUJ_D.		I-t T) \ \\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	_				
Improper Input Validation	16-10-201	.9 7.5	Office Laser have appli may	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary		N/A		H-HP-0 041119		
			CVE	ID : CVE	2019-6	334				
officejet_mar	naged_mfp_	x585_l3	u40a							
Improper Input Validation	16-10-201	9 7.5	Office Laser have appli may execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-0 041119	
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
officejet_ente	erprise_x555_c	2s11a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-OFFI- 041119/1924
officejet_ente	erprise_x555_c	2s12a		l	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-OFFI- 041119/1925
officiat ant	ammiss will l	1 h 4 F a			
omcejet_ente	erprise_x555_l	1n45a			T
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-OFFI- 041119/1926
			CVE ID : CVE-2019-6334		
pagewide_75	55_4pz47a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-PAGE- 041119/1927
CV Scoring Sca (CVSS)	o-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pub	lish Date	cvss	D	escription	n & CVE I	D	Pat	ch	NCIIP	C ID					
				code.												
				CVE	ID : CVE-	2019-6	334									
pagewide_en	iterpi	rise_76	5_j7z04a													
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu code.					H-HP-P. 041119							
					CVE ID : CVE-2019-6334											
pagewide_m	anage	ed_e751	160_j7z0	6a												
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A	H-HP-PAG 041119/1								
pagewide_m	anage	ed p753	250 v3z4													
pagewide_iii	T	zu_p/ 5/	230_y324		Ist T) \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	_									
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-P. 041119						
pagewide_m	anage	ed_mfp	p77440	y3z60a												
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			OfficeJet Enterprise, and LaserJet Managed Printers		7.5 OfficeJet Enterprise, and LaserJet Managed Printers		OfficeJet Enterprise, and LaserJet Managed Printers		N/A		H-HP-P. 041119	
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.				
			CVE ID : CVE-2019-6334				
pagewide_m	anaged_mfp_p	77940_	2gp22a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1932		
pagewide_m	 anaged_mfp_p'	77940 ₋					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1933		
pagewide_m	anaged_mfp_p'	77940 ₋					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1934		
pagewide_m	_ anaged_mfp_p'	77940 ₋					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-		
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	Pul	olish Date	cvss	D	escriptio	n & CVE I	D	P	atch	NCI	IPC ID
Input Validation				Laser have applie may a execu	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					04111	9/1935
pagewide_ma	anag	ed_mfp_	p77940	_5zn98	Ba						
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a	may allow potential execution of arbitrary		N/A		H-HP-1 04111	PAGE- 9/1936	
pagewide_ma	nnaa	od mfn	p77040			2019-0	334				
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.		N/A		H-HP- 04111	PAGE- 9/1937	
pagewide_ma	anag	ed mfn	p77940								
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP- 04111	PAGE- 9/1938	
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
pagewide_ma	anaged_mfp_p'	77940_	5zp01a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1939
pagewide_ma	anaged_mfp_p'	77940_	y3z61a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1940
nagewide m	 anaged_mfp_p'	77940			
pagewide_iii	anageu_mip_p	/ / 940_			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-PAGE- 041119/1941
			CVE ID : CVE-2019-6334		
pagewide_ma	anaged_mfp_p'	77940_	y3z63a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-PAGE- 041119/1942
CV Scoring Sca (CVSS)	o-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Puk	olish Date	CVSS	C	Description & CVE ID				tch	NCIIP	CID			
				code.										
				CVE	ID : CVE-	2019-6	334							
pagewide_m	anag	ed_mfp	p77940	_y3z64	ła									
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-PAG 041119/1				
pagewide_m	anag	ed_mfp	_p77940	_y3z65	y3z65a									
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		AGE- /1944			
					ID : CVE-	2019-6	334							
pagewide_m	anag	ed_mfp	_p77940	_y3z66	Sa									
Improper Input Validation	16-1	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				H-HP-P. 041119					
pagewide_m	anag	ed_mfp	p77940	_y3z68	_y3z68a									
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			OfficeJet Enterprise, and LaserJet Managed Printers		ceJet Enterprise, and erJet Managed Printers		N/A		H-HP-P. 041119	
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3					7-8	8-9	9-10			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			application signature that may allow potential execution of arbitrary code.					
			CVE ID : CVE-2019-6334					
pagewide_m	anaged_mfp_p'	77950_	2gp22a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1947			
pagewide_m	 anaged_mfp_p'	77950 ₋						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1948			
pagewide_m	_ anaged_mfp_p'	77950_						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1949			
pagewide_m	 anaged_mfp_p'	77950 ₋						
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-			
CV Scoring Sca (CVSS)	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	Pul	blish Date	cvss	D	escriptio	n & CVE I	D		Patc	h	NCIIF	CID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				041119	/1950
pagewide_ma	anag	ed_mfp	p77950	_5zn98	Ba							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Felet Enter Jet Mana a solution single ation of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A			H-HP-P 041119	
nagawida ma		ad mfm	~770F0		CVE ID : CVE-2019-6334							
pagewide_ma	anag	ea_mrp_	_p//950			YA7: 1						
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A			H-HP-P 041119	
				CVE I	D : CVE	2019-6	334					
pagewide_ma	anag	ed_mfp	p77950	_5zp00)a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A			H-HP-P 041119		
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
pagewide_ma	anaged_mfp_p'	77950_	5zp01a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1954
pagewide_ma	anaged_mfp_p'	77950	y3z61a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1955
nagowido m	 anaged_mfp_p'	77050			
pagewide_ini	mageu_mip_p	/ /950_		l	1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-PAGE- 041119/1956
			CVE ID : CVE-2019-6334		
pagewide_ma	anaged_mfp_p'	77950_	y3z63a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-PAGE- 041119/1957
CV Scoring Sca (CVSS)	o-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	Patc	h	NCIIP	CID
			code.				
			CVE ID: CVE-2019-6334				
pagewide_m	anaged_mfp_p	77950_	y3z64a	•			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A		H-HP-P 041119	
			CVE ID : CVE-2019-6334				
pagewide_m	anaged_mfp_p'	77950_	y3z65a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A		H-HP-P 041119	
pagewide_m	anaged_mfp_p	77950_	y3z66a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A		H-HP-P 041119	
pagewide_m	anaged_mfp_p	77950	y3z68a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A		H-HP-P. 041119	
CV Scoring Sco	ale 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 signature that may allow potential execution of arbitrary code.					
			CVE ID : CVE-2019-6334					
pagewide_m	anaged_mfp_p	77960_	2gp22a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1962			
pagewide_m	 anaged_mfp_p'	77960 ₋						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1963			
pagewide_m	_ anaged_mfp_p'	77960 ₋						
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1964			
pagewide_m	 anaged_mfp_p'	77960_	_2gp26a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-			
CV Scoring Sca (CVSS)	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	Pul	blish Date	cvss	D	escriptio	n & CVE I	D	ı	Patch		NCIIP	CID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				041119	/1965
pagewide_ma	anag	ed_mfp_	p77960	_5zn98	Ba							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Enter Jet Mana a solution single ation of a second control of a second con	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A			H-HP-P. 041119	
			77060		CVE ID : CVE-2019-6334							
pagewide_ma	anag	ea_m1p_	p//960			V.V. 1						
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A			H-HP-P. 041119	
				CVE I	D : CVE	-2019-6	334					
pagewide_ma	anag	ed_mfp_	p77960	_5zp00)a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A			H-HP-P. 041119		
CV Scoring Sca (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	Description & CVE ID	Patch	NCIIPC ID
pagewide_ma	anaged_mfp_p	77960	5zp01a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1969
pagewide_ma	anaged_mfp_p	77960	y3z61a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 041119/1970
lacariat anta	ernrico EOO mé	fn m E 7			
laserjet_ente	erprise_500_mf	ip_m52		T	1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1971
			CVE ID : CVE-2019-6334		
laserjet_ente	rprise_500_m	fp_m52	25f_cf118a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/1972
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	NCIIPC ID
			code.		
			CVE ID : CVE-2019-6334		
laserjet_ent	erprise_flow_m	fp_m5	25_cf116a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1973
			CVE ID : CVE-2019-6334		
laserjet_ent	erprise_flow_m	fp_m5	25_cf117a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1974
laserjet_ent	erprise_flow_m	fp_m5	25_cf118a		
Improper Input Validation 16-10-2019 7.5		7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1975
laserjet_mai	naged_500_mfp	_ m52 5	_l3u59a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1976
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.					
			CVE ID : CVE-2019-6334					
laserjet_man	aged_500_mfp	_m525	_l3u60a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1977			
laserjet_man	 aged_flow_mfj	p_m525	5_l3u59a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1978			
laserjet_man	 aged_flow_mfj	p_m525	5_13u60a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1979			
laserjet_ente	erprise_600_m	601_ce	 989a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-			
CV Scoring Sca (CVSS)	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	Puk	olish Date	cvss	D	escriptio	n & CVE I	& CVE ID		atch	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1980
laserjet_ente	rpris	se_600_1	m601_ce	990a							
Improper Input Validation	16-1	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Felet Enter Jet Mana solution singled allow position of a cut of the	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_ente	rpris	se 600 i	m602 ce								
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L 041119	
	_		100		D : CVE	2019-6	334				
Improper Input Validation	16-:	se_600_1		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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	D	escription	n & CVE II	D		Pato	h	NCIIF	CID
laserjet_ente	rprise_600_m	602_ce	993a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334							H-HP-L 041119	
laserjet_ente	rprise_600_m	603_ce	991a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-LASE- 041119/1985	
laserjet_ente	rprise_600_m	603_ce	992a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	serJet, Post Enter Jet Mana a solution signation of a	rprise, a aged Prin on to che gnature tential orbitrary	nd nters ock that	N/A			H-HP-L 041119	
lacariat anta	rprise_600_m	603 co		D. GIL	2017 0	55 1					
iaserjet_ente		oos_ce		ıserJet, P	ageWid	e,					
Improper Input Validation	16-10-2019	7.5	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A			H-HP-L 041119	
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	
			code.			
			CVE ID : CVE-2019-6334			
laserjet_ente	erprise_700_mi	fp_m77	′5_cc522a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1988	
lacariat auto		fra va 77				
laserjet_ente	erprise_700_mf	rp_m / /		I		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/1989	
			CVE ID : CVE-2019-6334			
laserjet_ente	erprise_700_mi	tp_m77	/5_cc524a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1990	
laserjet_ente	erprise_700_m	fp_m77	75_cf304a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/1991	
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.								
			CVE ID : CVE-2019-6334								
laserjet_ente	erprise_700_m	fp_m77	75_l3u49a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1992						
laserjet_ente	erprise_700_m	fp_m77	/5_l3u50a								
Improper Input Validation	at 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1993						
laserjet_man	laged_mfp_m7'	75_cc5									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/1994						
laserjet_man	laserjet_managed_mfp_m775_cc523a										
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-						
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	C ID
Input Validation				Laser have applie may a execu- code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/1995
laserjet_man	aged	l_mfp_m	1775_cc5	24a							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
laserjet_man	aged	l_mfp_m	1775_cf3	04a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Felet Enter Jet Mana solution single ation of a tion of a series.	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_man	aged	l mfn m	775 l3u								
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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	D	escription	n & CVE II	D		Pato	h	NCIIP	C ID
laserjet_man	aged_mfp_m7	75_l3u	50a								
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	serJet, PeJet Enter Jet Mana a solutio cation signallow pot ation of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/	'A		H-HP-L. 041119	
laserjet_ente	rprise_700_m	712_cf	235a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-L. 041119	
laseriet ente	rprise_700_m	712 cf									
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				'A		H-HP-L. 041119	
laserjet_ente	rprise_700_m	712_cf	238a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/	'A		H-HP-L. 041119	
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	
			code.			
			CVE ID : CVE-2019-6334			
laserjet_ente	erprise_flow_m	fp_m63	30_b3g86a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/2003	
			CVE ID : CVE-2019-6334			
laserjet_ente	erprise_flow_m	fp_m63	30_13u62a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2004	
lacariat ante	mariae flerr m	for ma 6'				
laserjet_ente	erprise_flow_m	тр_ть.				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2005	
laserjet_ente	erprise_flow_m	fp_m63	30_p7z48a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	H-HP-LASE- 041119/2006		
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_ente	rprise_mfp_m	630_b3	g84a	<u> </u>	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2007
laserjet_ente	rprise_mfp_m	630_b3	g85a		
Improper Input Validation	Input 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2008
laseriet ente	rprise_mfp_m	630 i7			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2009
laserjet_ente	rprise_mfp_m	630_l3	u61a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ole 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	D	escriptio	n & CVE I	D	Pa	tch	NCIIF	CID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po tion of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/2010
laserjet_man	aged	l_flow_n	1fp_m63	0_b3g8	86a						
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
laserjet_man	2000	l flow n	ofn m63			2017-0	JJT				
iasei jet_iiidii	ageu		nh_mos			Dago[M: 4	0				
Improper Input Validation	16-10-2019 7.5				HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.					H-HP-L 041119	
					D : CVE-	·2019-6	334				
laserjet_man	aged	l_flow_n	nfp_m63	0_p7z4	7a						
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
laserjet_man	aged_flow_mf	p_m63	0_p7z4	∙8a						
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a nged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_m6	30_b3g	84a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_m6	30_b3g	85a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L. 041119	
laseriet man	aged_mfp_m6	30 j7x2	 28a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L. 041119	
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	Pul	olish Date	CVSS	D	escriptio	n & CVE I	D	Pa	Patch		CID
				code.							
				CVE	ID : CVE	2019-6	334				
laserjet_mar	aged	l_mfp_m	1630_l3u	61a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a	aserJet, FeJet Ente Jet Mana a solutio cation si allow po ation of a	rprise, and aged Price of the character	nters eck that	N/A		H-HP-L. 041119	
				CVE	ID : CVE	2019-6	334				
laserjet_ente	erpris	se_flow_	mfp_m8	30_cf3	67a						
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		H-HP-LASE- 041119/201	
1		G	f O		ID : CVE-	2019-6	334				
laserjet_ente	erpris	se_flow_	mrp_m8								
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_mar	aged	l_flow_n	nfp_m83	0_cf36	7a						
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			N/A		H-HP-LASE- 041119/2021		
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	3-4 4-5 5-6		5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			application signature that may allow potential execution of arbitrary code.		
			CVE ID: CVE-2019-6334		
laserjet_man	aged_flow_mfp	o_m830)_l3u65a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2022
laserjet_ente	rprise_m4555	_mfp_c	e502a		•
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2023
laserjet_ente	rprise_m4555	_mfp_c	e503a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2024
laserjet_ente	rprise_m4555	_mfp_c	e504a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
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	Pu	blish Date	cvss	D	escriptio	n & CVE I	D		Patc	h	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				041119)/2025
laserjet_ente	rpri	se_m45	55_mfp_0	ce738a	l							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-L 041119	
laserjet_ente	rpri	se_m50	6_f2a66a	l								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.						H-HP-L 041119	
laserjet_ente	rnri	se m50	6 f2a67a		D I GVE							
Improper Input Validation		10-201 9		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A			H-HP-L 041119		
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
laserjet_ente	rprise_m506_f	f2a68a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2029
laserjet_ente	rprise_m506_f	f2a69a		1	1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2030
laseriet ente	rprise_m506_f	f2a70a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2031
lagariat anto	movice mcCOC	Ma71a			
laserjet_ente	rprise_m506_f	12a/1a	HP LaserJet, PageWide,		
Improper Input Validation	16-10-2019	7.5	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/2032
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	D	escriptio	n & CVE I	D	Pato	h	NCIIP	CID
			code.							
			CVE I	D : CVE-	2019-6	334				
laserjet_mar	aged_m506_f	2a66a								
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L. 041119	
laseriet mar	laged_m506_f	2a67a	CVL 1D . CVL 2017 0334							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_mar	naged_m506_f	2a68a								
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334		N/A		H-HP-L. 041119		
laserjet_mar	aged_m506_f	2a69a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check				N/A		H-HP-L. 041119	
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_man	aged_m506_f2	a70a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2037
laserjet_man	aged_m506_f2	a71a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2038
laserjet_ente	rprise_m507_1	1pu51a	1		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2039
laserjet_ente	rprise_m507_1	1pu52a	1 1		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
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	D	escriptio	n & CVE II	D	Pat	ch	NCIIP	C ID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pring n to che gnature tential arbitrary	nters ck that			041119	/2040
laserjet_ente	rprise_m507_	1pv86a	a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	_
laserjet_ente	rprise_m507_	1pv87a	3							
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu code.	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Prin n to che gnature tential arbitrary	nd nters ck that	N/A		H-HP-L. 041119	
		1 00		D : CVE-	2019-6	334				
laserjet_ente	rprise_m507_	1pv88a		ıserJet, F	Date Miss	0				
Improper Input Validation	16-10-2019	7.5	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
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	D	escription	n & CVE II	D		Pato	h	NCIIF	C ID
laserjet_ente	rprise_m507_	1pv89a	a								
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Post Enter Jet Mana a solution cation signallow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/A	A		H-HP-L 041119	
laserjet_man	aged_e50145_	1pu51	a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-L 041119	
laserjet_man	aged_e50145_	1pu52	a								
Improper Input Validation	16-10-2019	7.5	HP La Office Laser have applie may a execu	serJet, Poset Enter Jet Mana a solution cation signallow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/A	Α		H-HP-L 041119	
laserjet_man	aged_e50145_	1pv86	a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A	A		H-HP-L 041119	
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	Pub	lish Date	cvss	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	C ID	
				code.								
				CVE I	D : CVE-	2019-6	334					
laserjet_man	aged	_e5014	5_1pv87	a								
Improper Input Validation	16-2	10-2019	7.5	Office Laser have appli- may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID : CVE-2019-6334 HP LaserJet, PageWide,					H-HP-LASE 041119/20		
1		-5014	T 100									
laserjet_man	aged	_e5014	5_1pv88		P Laserlet PageWide							
Improper Input Validation	16-2	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L ₂ 041119	_	
laserjet_man	aged	e5014	5 1pv89	<u> </u> а								
laser jet_man	lageu	_63014	J_TPVO		ngorlot F	DagoWid	0					
Improper Input Validation	16-2	10-2019	7.5	Office Laser have appli- may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L ₂ 041119		
laserjet_ente	erpris	e_m604	4_e6b67a	'a								
Improper Input Validation	16-2	10-2019	7.5 HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			OfficeJet Enterprise, and LaserJet Managed Printers				H-HP-L		
CV Scoring Sca	ale	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	D	escription	n & CVE I	D	Pato	h	NCIIP	C ID
				may a	cation signallow potention of a	tential					
				CVE I	D : CVE-	2019-6	334				
laserjet_ente	rpris	e_m604	1_e6b68	a							
Improper Input Validation	16-1	10-2019	7.5					N/A		H-HP-LA 041119	
laserjet_ente	rpris	e m60!	5 e6b69a								
Improper Input Validation	16-1	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-LA 041119	
laserjet_ente	rpris	e_m60	5_e6b70	_							
Improper Input Validation	16-1	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-LA 041119	
laserjet_ente	rpris	e_m60	5_e6b71	la							
Improper	16-1	10-2019	7.5	HP LaserJet, PageWide,			N/A		H-HP-L	ASE-	
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	Pu	blish Date	cvss	D	escriptio	n & CVE I	D	Pa	atch	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/2055
laserjet_ente	rpri	se_m60	5_l3u53a		.2						
Improper Input Validation	-	10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L 041119	
laserjet_ente	rpri	se_m60	5_l3u54a	1							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Felet Enter Jet Mana solution singled allow position of a section of a sect	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_ente	rpri	se m60	6 e6b72								
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
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	D	escription	n & CVE I	D	Pa	itch	NCIIP	CID
laserjet_ente	rprise_m606_	e6b73a	a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	IserJet, Post Enter Jet Mana a solution signification of a discourse of a discourse of the control of a discourse of a discour	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_man	aged_m605_e	6 b 69a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_m605_e	6 b 70a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	serJet, Pet Enter Jet Mana a solution cation signallow por tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laseriet man	aged_m605_e	6h71a	0.21							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L. 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	1	NCIIP	CID
			code.				
			CVE ID: CVE-2019-6334				
laserjet_mar	naged_m605_l3	u53a				<u> </u>	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A		H-HP-LASE- 041119/2063	
	1 (05 10	= 4	CVE ID : CVE-2019-6334				
laserjet_mai	naged_m605_l3	u54a				T.	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A		H-HP-L. 041119	
laserjet_ent	erprise_m607_l	k0q14a	1				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A		H-HP-L 041119	
laserjet_ent	erprise_m607_l	k0q15a	1				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A		H-HP-L 041119	
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID: CVE-2019-6334		
laserjet_ente	rprise_m608_l	k0q17a	l		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2067
laserjet_ente	rprise_m608_l	k0q18a	1		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2068
laserjet_ente	rprise_m608_l	k0q19a	1		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2069
laserjet_ente	rprise_m608_1	m0p32	a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
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	Pul	blish Date	cvss	D	escriptio	n & CVE I	D		Patc	h	NCIIF	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				041119	/2070
laserjet_ente	rpri	se_m609	9_k0q20		-							
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A			H-HP-L 041119	
laserjet_ente	rpri	se_m609	9_k0q21	a								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	serJet, Fet Enter Jet Mana a solution single grant on the section of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A			H-HP-L 041119	
laserjet_ente	rnri	se m609	9 k0a22									
Improper Input Validation	-	10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-L 041119	
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	·				Pat	tch	NCIIP	C ID
laserjet_man	aged_e60075_	m0p33	3a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/A		H-HP-L. 041119	
laserjet_man	aged_e60075_	m0p35	5a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
laserjet_man	aged_e60075_	_m0p36	óa							
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary		N/A		H-HP-L. 041119		
laseriet man	aged_e60075_	m0n39								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			nd nters ck that	N/A		H-HP-L. 041119	
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	Pul	blish Date	e CVSS	·					atch	NCIII	PCID
				code.							
				CVE	ID : CVE-	2019-6	334				
laserjet_man	aged	l_e6007	5_m0p4	0a							
Improper Input Validation	16-	10-2019	7.5	may allow potential execution of arbitrary code. CVE ID : CVE-2019-6334				N/A		H-HP-L 041119	_
lacariat anto		00 m00	6 072446								
laserjet_ente	erpris	se_m80	6_CZZ448					-			
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	
laserjet_ente	erpris	se_m80	6_cz245a	<u> </u>							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
laserjet_ente	erpri	se_flow_	_mfp_m5	527z_f2a76a							
Improper Input Validation	16-	10-2019	Office Let Enterprise and		LaserJet Managed Printers			N/A		H-HP-L 041119	
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_ente	erprise_flow_m	fp_m52	27z_f2a77a		1
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2082
laserjet_ente	erprise_flow_m	fp_m52	27z_f2a78a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2083
laserjet_ente	erprise_flow_m	fp_m52	27z_f2a81a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2084
laserjet ente	erprise_mfp_m	527_f2			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pul	olish Date	cvss	OfficeJet Enterprise, and				F	Patch	NCIIP	CID
Input Validation				Laser have applie may a execu- code.	elet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/2085
laserjet_ente	rpris	se_mfp_	m527_f2	a77a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-L. 041119	
laserjet_ente	rpris	se_mfp_i	m527_f2	a78a							
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.					H-HP-L. 041119	
lagariat anto	un ui		m [27 f]		D : CVE	-2019-0	0334				
Improper Input Validation	-	10-2019		HP La Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L. 041119	
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	D	escription	n & CVE I	D	Pat	ch	NCIIP	C ID
laserjet_man	aged_flow_mfj	p_m52	7z_f2a'	79a						
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	IserJet, Polet Ente Jet Mana a solutio cation signallow pol tion of a	rprise, a nged Prin n to che gnature tential nrbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_man	aged_flow_mfj	p_m52′	7z_f2a80a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_m5	27_f2a	79a							
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.					H-HP-L. 041119	
laseriet man	aged_mfp_m5	27 f2a	80a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L. 041119	
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	Pu	blish Date	e CVSS	·				Pat	tch	NCIIF	PC ID	
				code.								
				CVE	ID : CVE	-2019-6	334					
laserjet_ente	rpri	se_mfp_	m528_1	ps54a						L		
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu						H-HP-L 041119		
					ID : CVE	-2019-6	334					
laserjet_ente	erpri	se_mfp_	m528_1	ps55a								
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119	_	
laserjet_ente	erpri	se mfp	m528 1	pv49a								
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L 041119		
laserjet_ente	erpri	se_mfp_	m528_1	pv64a								
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			and nters	N/A		H-HP-L 041119		
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_ente	erprise_mfp_m	528_1p	v65a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2097
laserjet_ente	erprise_mfp_m	528_1p	v66a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2098
laserjet_ente	erprise_mfp_m	528_1p	 v67a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2099
laserjet_man	aged_mfp_e52	645_1 ₁	os54a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
CV Scoring Sca (CVSS)	ole 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Da	ate C\	/SS	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
Input Validation				Laser have a applie may a execu code.	Jet Mana a solutic cation si allow po tion of a	ırbitrary	nters eck that			041119	/2100
laserjet_man	aged mfn	e52645	5 1n	CVE ID : CVE-2019-6334							
Improper Input Validation	16-10-202			HP La Office Laser have a applie may a execu	Jet Ente Jet Mana a solution cation si Illow po tion of a	PageWid rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_	e52645	5_1p	v49a							
Improper Input Validation	16-10-203	19 7.	5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		H-HP-L. 041119	
laserjet_man	aged mfn	e52645	5 1p			-2019-6					
Improper Input Validation	16-10-202			HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
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	D	escription	n & CVE II	D		Pato	h	NCIIP	CID
laserjet_man	aged_mfp_e52	645_1 _]									
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	serJet, Post Enter Jet Mana a solution cation signallow pot tion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/	A		H-HP-L. 041119	
laserjet_man	aged_mfp_e52	645_1 _]	pv66a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/	A		H-HP-L. 041119	
lacariat man	agod mfn o52	CVE ID : CVE-2019-6334 52645_1pv67a									
laserjet_man	ageu_mrp_e52	045_1		• •							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/	A		H-HP-L. 041119	
_	_	-		D : CVE-	2019-6	334					
laserjet_ente	rprise_flow_m	fp_m6									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			nd nters ck that	N/	A		H-HP-L. 041119	
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	Pul	blish Date	CVSS	D	escriptio	n & CVE I	D	Pat	ch	NCIIP	C ID
				code.							
				CVE	D : CVE	2019-6	334				
laserjet_ente	erpris	se_flow_	mfp_m6	31_j8j	64a						
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu code.		rprise, a aged Pri on to che gnature tential arbitrary	and nters eck that	N/A		H-HP-L. 041119	_
				CVE ID : CVE-2019-6334 31_j8j65a							
laserjet_ente	erpris	se_flow_	mfp_m6	. ,							
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	_
lacariet ente		as flow				-2019-0	0334				
laserjet_ente	erpris	se_now_	тр_ть						ı		
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119	_	
laserjet_ente	erpris	se_flow_	mfp_m6	32_j8j71a							
Improper Input Validation	16-	10-2019	Office Let Enterprise and			LaserJet Managed Printers				H-HP-L 041119	
CV Scoring Sca (CVSS)	ale	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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	C ID
				may a	cation signallow potential	tential					
				CVE I	D : CVE-	2019-6	334				
laserjet_ente	rpris	e_flow_	mfp_m6	32_j8j7	72a						
Improper Input Validation	16-1	10-2019	7.5	Office Laser have applie may a execu- code.	eserJet, Pelet EnterJet Mana a solution signallow portion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-LA 041119	
laserjet_ente	rpris	e_flow_	mfp_m6								
Improper Input Validation	16-1	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-LA 041119	
laserjet_ente	rpris	e_flow_	mfp_m6	33_j8j7	78a						
Improper Input Validation	16-1	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-LA 041119	
laserjet_ente	rpris	e_mfp_	m631_j8	8j63a							
Improper	16-1	10-2019	7.5	HP LaserJet, PageWide,			N/A		H-HP-L	ASE-	
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	OfficeJet Enterprise, and					atch	NCIIP	CID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solutio cation si allow po tion of a	aged Pring In to che gnature tential Inbitrary	nters ock that			041119	/2115
laserjet_ente	rprise_mfp_m	631_j8	j64a							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_ente	rprise_mfp_m	631_j8	j65a							
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary			N/A		H-HP-L. 041119	
				D : CVE-	2019-6	334				
laserjet_ente	rprise_mfp_m	632_j8								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119		
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	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
laserjet_ente	rprise_mfp_m	632_j8	j71a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a aged Prin on to che gnature tential orbitrary	nd nters ock that	N/A		H-HP-L. 041119	
laserjet_ente	rprise_mfp_m	632_j8	j72a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L 041119	
laserjet_ente	rprise_mfp_m	633_j8	j76a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L 041119	
lacariat anta	rnrico mfn m	622 (0		D. CVE	2017-0	JJT				
laserjet_ente	rprise_mfp_m	uss_jø		sarlot D	PagoMid	Δ				
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a	serJet, Pet Ente Jet Mana a solutio cation signation of a	rprise, a aged Prin on to che gnature tential	nd nters ck that	N/A		H-HP-L. 041119	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			code.								
			CVE ID: CVE-2019-6334								
laserjet_mai	naged_flow_mfp	o_e625	55_j8j66a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/2123						
				CVE ID : CVE-2019-6334							
laserjet_mai	naged_flow_mfp	o_e625	55_j8j67a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2124						
laserjet_mai	naged_flow_mfp	e625	55_j8j73a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2125						
laserjet_mai	naged_flow_mfp	o_e625	55_j8j74a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/2126						
CV Scoring Sc (CVSS)	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						
			application signature that may allow potential execution of arbitrary code.								
			CVE ID : CVE-2019-6334								
laserjet_man	aged_flow_mfj	p_e625	55_j8j79a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2127						
laserjet_managed_flow_mfp_e62555_j8j80a											
Improper Input Validation	mproper nput 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2128						
laserjet_man	aged_flow_mfj	p_e625	65_j8j66a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2129						
laserjet_man	 aged_flow_mf	o_e625									
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-						
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	D	escriptio	n & CVE I	D	Pa	tch	NCIIP	CID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solutio cation si allow po tion of a	aged Pring In to che gnature tential Inbitrary	nters ock that			041119	/2130
laserjet_man	aged_flow_mfp	o_e625	65_j8j	73a						
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu code.	serJet, Fet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Prin on to che gnature tential arbitrary	nd nters ock that	N/A		H-HP-L. 041119	
1	1 GC	625		D : CVE-	2019-6	334				
laserjet_man	aged_flow_mfp)_e625			YAT: 1					
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a	Jet Mana a solutio cation si allow po	rprise, a aged Prin on to che gnature tential	nd nters ck that	N/A		H-HP-L 041119	
			CVE I	D : CVE-	2019-6	334				
laserjet_man	aged_flow_mfp	o_e625	65_j8j	79a						
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	EVE ID: CVE-2019-6334 5_j8j79a HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check pplication signature that hay allow potential execution of arbitrary			N/A		H-HP-L 041119	
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
laserjet_man	aged_flow_mfp	e625	65_j8j80a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2134
laserjet_man	aged_flow_mfp	_e625	75_j8j66a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2135
		60.			
laserjet_man	aged_flow_mfp	o_e625	75_j8j67a 	,	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/2136
			CVE ID : CVE-2019-6334		
laserjet_man	aged_flow_mfp	o_e625	75_j8j73a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/2137
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	Patcl	h	NCIIF	PC ID					
			code.									
			CVE ID: CVE-2019-6334									
laserjet_mar	naged_flow_mfp	o_e625	75_j8j74a									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A		H-HP-LASE- 041119/2138						
			CVE ID: CVE-2019-6334									
laserjet_managed_flow_mfp_e62575_j8j79a												
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A		H-HP-L 041119						
laserjet_mai	naged_flow_mfp	e625	75_j8j80a									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334		N/A		ASE- 0/2140					
laserjet_mai	naged_mfp_e62	555_j8	j66a									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		H-HP-LASE- 041119/2141							
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.								
			CVE ID : CVE-2019-6334								
laserjet_man	aged_mfp_e62	555_j8	j67a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2142						
laserjet_managed_mfp_e62555_j8j73a											
Improper Input Validation	Improper Input 16-10-2019 7.5		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2143						
laseriet man	aged_mfp_e62	555 i8									
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2144						
laserjet_man	aged_mfp_e62	555_j8	j79a		•						
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-						
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	D	escriptio	n & CVE I	D	Pa	tch	NCIIP	CID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solutio cation si allow po tion of a	aged Pring In to che gnature tential Inbitrary	nters ck that			041119	/2145
laserjet_man	aged_mfp_e62	555_j8	ij80a							
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu code.	serJet, Fet Ente Jet Mana a solution cation si allow po- tion of a	rprise, a aged Prin on to che gnature tential orbitrary	nd nters ck that	N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_e62	565_j8								
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a	Jet Ente Jet Mana a solutio cation si allow po	PageWide, terprise, and naged Printers ion to check signature that otential Farbitrary		H-HP-L. 041119			
				D : CVE-	2019-6	334				
laserjet_man	aged_mfp_e62	565_j8								
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu- code.	serJet, F Jet Ente Jet Mana a solution cation si allow po tion of a	rprise, a aged Prin on to che gnature tential arbitrary	nd nters ck that	N/A		H-HP-L. 041119	
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	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
laserjet_man	aged_mfp_e62	565_j8	j73a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a aged Prin n to che gnature tential rbitrary	nd nters ck that	N/A		H-HP-L. 041119	
laserjet_man	aged_mfp_e62	565_j8	j74a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.					H-HP-L. 041119	
laserjet_man	aged_mfp_e62	565_j8	j79a							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary					H-HP-L. 041119	
lacariat man	aged_mfp_e62	565 i8		D.CVL	2017 0	JJ 1				
laser jet_illali	ageu_mp_e02	,303_J0		ıserlet. P	ageWid	e.				
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a	may allow potential execution of arbitrary code. CVE ID : CVE-2019-6334 79a HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID : CVE-2019-6334 80a HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check				H-HP-L. 041119		
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Pul	blish Date	e CVSS	D	escriptio	n & CVE I	D	Pate	ch	NCIIP	C ID	
				code.								
				CVE	ID : CVE	2019-6	334					
laserjet_ente	erpris	se_mfp_	m725_cf	066a								
Improper Input 16-1 Validation		10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-LASE- 041119/215		
					ID : CVE-	2019-6	334					
laserjet_ente	erpris	se_mfp_	m725_cf	067a								
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				H-HP-LASE 041119/21		_	
lacariat ante			m725 of		ID : CVE	-2019-0	334					
laserjet_ente	erpris	se_mrp_	m725_ci	_					T			
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119		
laserjet_ente	erpris	se_mfp_	m725_cf	069a								
Improper Input Validation	16-	10-2019	7.5	Office Laser	omeejee Enterprise, and N/A			H-HP-L. 041119				
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	3-4	3-4 4-5 5-6 6-7 7-8		8-9	9-10			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID						
			application signature that may allow potential execution of arbitrary code.								
			CVE ID : CVE-2019-6334								
laserjet_ente	erprise_mfp_m	725_l3	u63a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2157						
laserjet_enterprise_mfp_m725_l3u64a											
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2158						
laserjet_man	aged_mfp_m7	25_cf06	56a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2159						
laserjet_man	 aged_mfp_m7	25_cf0 <i>6</i>	57a								
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-						
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	Pu	blish Date	CVSS	D	escriptio	n & CVE I	D	P	atch	NCIIF	PC ID
Input Validation				Laser have applie may a execu	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					041119	0/2160
laserjet_cm4	540 _	_mfp_cc4	119a								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu	aserJet, For the Jet Mana a solution single allow position of a section of a section single.	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
laserjet_cm4	540_	mfp_cc4	120a								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a	may allow potential execution of arbitrary code.		H-HP-L 041119				
laserjet_cm4	540 ₋	mfp_cc4	121a								
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	aserJet, Felet Enter Jet Mana a solution single ation of a tion of a column.	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L 041119	
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
laserjet_ente	erprise_flow_m	fp_m8	80z_a2w75a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2164
laserjet_ente	erprise_flow_m	fp_m8	80z_a2w76a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2165
locariot anto	rprise_flow_m	fn m0			
laserjet_ente	erprise_now_m	ıp_mo		l	<u> </u>
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/2166
			CVE ID : CVE-2019-6334		
laserjet_ente	erprise_flow_m	fp_m8	80z_d7p71a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/2167
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	NCIIPC ID
			code.		
			CVE ID : CVE-2019-6334		
laserjet_ente	erprise_flow_m	fp_m8	80z_l3u51a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/2168
			CVE ID : CVE-2019-6334		
laserjet_ente	erprise_flow_m	fp_m8	80z_l3u52a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2169
laserjet_man	 naged_flow_mfp	_m88(Dzm_a2w75a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2170
laserjet_man	naged_flow_mfp	o_m880	Ozm_a2w76a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/2171
CV Scoring Sca (CVSS)	ale 0-1	6-7 7-8	8-9 9-10		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			application signature that may allow potential execution of arbitrary code.			
			CVE ID : CVE-2019-6334			
laserjet_man	aged_flow_mfj	_m88(Ozm_d7p70a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2172	
laserjet_man	aged_flow_mfj	p_m880	Dzm_d7p71a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2173	
laserjet_man	aged_flow_mfj	_m880	Ozm_l3u51a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2174	
laserjet_man	 aged_flow_mfj		Dzm_l3u52a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-	
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	D	escriptio	n & CVE II	D	Pate	ch	NCIIP	CID
Input Validation			Laser have applie may a execu code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pring on to che gnature tential arbitrary	nters ck that			041119	/2175
laserjet_ente	rprise_m552_	b5l23a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A		H-HP-L. 041119	
laserjet_ente	rprise_m553_	b5l24a								
Improper Input Validation	16-10-2019	7.5	Office Laser have applie may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L. 041119	
lacariet ente	rprise_m553_	h5125a		D : CVE-	2019-0	334				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119		
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	D	escription	n & CVE II	D	F	Patch	NCIIF	PC ID
laserjet_ente	rprise_m553_	b5l26 a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	IserJet, Post Enter Jet Mana a solution signallow postion of a	rprise, a aged Prin on to che gnature tential orbitrary	nd nters ck that	N/A		H-HP-L 041119	
laserjet_ente	rprise_m553_	b5l38 a	1							
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334					H-HP-L 041119	
laserjet_ente	rprise_m553_	b5l39 a	1						•	
Improper Input Validation	16-10-2019	7.5	Office Laser have a applie may a execu code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.			N/A		H-HP-L 041119	
lacariat anta	mnnico mEE2	h127a	CVEI	D : CVE-	2019-0	JJ4				
laserjet_ente	rprise_m553_	DIZ/a	ם מען	ıserJet, P	Date Miss	0				
Improper Input Validation	16-10-2019	7.5	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary				N/A		H-HP-L 041119	
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	D	escriptio	n & CVE I	D	Pato	:h	NCIIP	CID
			code.							
			CVE I	D : CVE-	2019-6	334				
laserjet_mar	aged_m553_b	5124a								
Improper Input Validation	16-10-2019	7.5	Office Laser have a applic may a execu code.	IserJet, Forter Enter Jet Mana a solution singled tion of a	rprise, a aged Pri on to che gnature tential arbitrary	nnd nters eck that	N/A		H-HP-L. 041119	
lacariat mar	laged_m553_b	51252	CVE ID : CVE-2019-6334							
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L. 041119		
laserjet_mar	aged_m553_b	5126a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334		N/A		H-HP-L. 041119			
laserjet_mar	aged_m553_b	5138a								
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check			N/A		H-HP-LASE- 041119/2186		
CV Scoring Sca (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID: CVE-2019-6334		
laserjet_man	aged_m553_b	5139a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2187
laserjet_man	aged_m553_bl	27a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2188
laserjet_ente	rprise_m651_c	cz255a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2189
laserjet_ente	rprise_m651_0	cz256a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-
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	Pu	blish Date	e CVSS	D	escriptio	n & CVE I	& CVE ID		atch	NCIIF	C ID
Input Validation				Laser have applie may a execu- code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			041119	/2190
laserjet_ente	rpri	se_m65	1_cz257	a a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	may allow potential execution of arbitrary			N/A		H-HP-L 041119	
laserjet_ente	rpri	se_m65	1_h0dc9	a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.					H-HP-L 041119	
laserjet_ente	rnri	se m65	1 18707:		2.011						
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			N/A		H-HP-L 041119		
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
laserjet_man	aged_m651_cz	255a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2194
laserjet_man	aged_m651_cz	256a		1	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2195
laseriet man	aged_m651_cz	257a	CVE15 : CVE 2017 0301		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2196
laseriet man	aged_m651_h(Odc9a	0.2.2.0.2.20.2		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-LASE- 041119/2197
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	NCIIPC ID
			code.		
			CVE ID : CVE-2019-6334		
laserjet_mai	naged_m651_l8	z07a			'
Improper Input 16-10-2019 7.5 Validation			HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-LASE- 041119/2198
			CVE ID : CVE-2019-6334		
laserjet_ento	erprise_m652_j	7z98a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2199
laserjet_ent	erprise_m652_j	7z99a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 041119/2200
laserjet_ent	erprise_m653_j	j8a04a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A	H-HP-LASE- 041119/2201
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
laserjet_ente	rprise_m653_j	8a05a			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-LASE- 051119/2202
pagewide_ma	 anaged_mfp_p'	77960_	_y3z62a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2203
pagewide_ma	 anaged_mfp_p'	77960 ₋	y3z63a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2204
pagewide_ma	 anaged_mfp_p'	77960 ₋			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-
CV Scoring Sca (CVSS)	lle 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	D	escriptio	n & CVE I		Patcl	า	NCIIP	CID	
Input Validation				Laser have applie may a execu- code.	OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334						051119	/2205
pagewide_ma	anag	ed_mfp	p77960	_y3z65	a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	may allow potential execution of arbitrary			N/A			H-HP-P 051119	
pagewide_ma	anao	ed mfn	n77960			2017 0	,33 1					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.						H-HP-P 051119	
pagewide_ma	nnaa	ad mfn	n77060			-2019-0	334					
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP-P 051119	
CV Scoring Sca (CVSS)	le	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
pagewide_m	fp_774_4pa44a	ì			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2209
pagewide_m	fp_774_4pz43a	l			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2210
pagewide_m	 fp_779_4pz45a	<u> </u>			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2211
pagewide m	 fp_779_4pz46a	1			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-PAGE- 051119/2212
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	1	NCIIP	CID
			code.				
			CVE ID: CVE-2019-6334				
pagewide_er	nterprise_556_	g1w46	a				
Improper Input 16-10-2019 Validation		7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A		H-HP-P. 051119	
	CVE ID : CVE-2019-6334						
pagewide_ei	nterprise_556_	g1w46				I	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A		H-HP-P. 051119	
pagewide_ei	nterprise_556_	g1w47	a				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	t N/A		H-HP-PA 051119/	
pagewide_en	nterprise_556_	g1w47	v				
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	N/A		H-HP-P. 051119	
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
pagewide_m	anaged_e5565	0_l3u4	4 a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2217
pagewide_en	terprise_flow_	mfp_7	80f_j7z09a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2218
pagewide_en	 terprise_flow_	mfp_78	 80f_j7z10a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2219
pagewide_en	 terprise_flow_	mfp_78	 85_j7z11a		
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	F	Patch		NCIIP	C ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that			(051119	/2220
pagewide_en	terp	rise_flov	w_mfp_7	85_j7z	12a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334		N/A			H-HP-P/ 051119		
pagewide_en	tern	rise mfi	n 780 i7									
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.		N/A			H-HP-PA 051119		
nagawida an	tonn	nico mf	n 700 i7		D:CVE	-2019-0	0334					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary						H-HP-PA 051119	
CV Scoring Sca (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	Description & CVE ID	Patch	NCIIPC ID
pagewide_ma	anaged_flow_n	1fp_e7	7650_j7z05a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2224
pagewide_ma	anaged_flow_n	ıfp_e7	7650_j7z08a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2225
nagewide ma	 anaged_flow_n	1fn e7'			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-PAGE- 051119/2226
		_	CVE ID : CVE-2019-6334		
pagewide_ma	anaged_flow_n	1fp_e77	·		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-PAGE- 051119/2227
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	Patc	h	NCIIP	PC ID	
			code.					
			CVE ID : CVE-2019-6334					
pagewide_m	anaged_flow_n	nfp_e77	7650_z5g79a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A		H-HP-PAGE- 051119/222		
			CVE ID : CVE-2019-6334					
pagewide_m	anaged_flow_n	nfp_e77	7660z_j7z03a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A		H-HP-PAGE- 051119/2229		
pagewide_m	anaged_flow_n	nfp_e77	7660z_j7z05a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	PageWide, terprise, and naged Printers ion to check signature that otential f arbitrary			AGE- 1/2230	
pagewide_m	anaged_flow_n	nfp_e77	7660z_j7z07a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check	nterprise, and n/A anaged Printers			H-HP-PAGE- 051119/2231	
CV Scoring Sc (CVSS)	ale 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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
pagewide_m	anaged_flow_n	ıfp_e77	7660z_j7z08a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2232
pagewide_m	anaged_flow_n	nfp_e77	7660z_j7z13a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2233
pagewide_m	anaged_flow_n	1fp_e77	7660z_j7z14a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2234
pagewide_m	 anaged_flow_n	1fp_e77			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-
CV Scoring Sca (CVSS)	ale 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	D	escriptio	n & CVE I	D	ı	Patch		NCIIP	CID
Input Validation				Laser have applie may a execu- code.	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				051119	/2235
pagewide_ma	anag	ed_flow	_mfp_e7	7660z	_z5g79a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	may allow potential execution of arbitrary					H-HP-P. 051119		
pagewide_ma	anag	ed_mfp_	e77650	_j7z05a	a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.		N/A			H-HP-P. 051119		
		d C	-77(50		D : CVE	-2019-6	334					
Improper Input Validation		10-2019		HP La Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary						H-HP-P. 051119	
CV Scoring Sca (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	Description & CVE ID	Patch	NCIIPC ID
pagewide_ma	anaged_mfp_e	77650_	j7z13a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2239
pagewide_ma	anaged_mfp_e	77650_	j7z14a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2240
nagewide ma	 anaged_mfp_e'	77650			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.	N/A	H-HP-PAGE- 051119/2241
			CVE ID : CVE-2019-6334		
pagewide_en	terprise_flow_	mfp_5			
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary	N/A	H-HP-PAGE- 051119/2242
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	Pul	blish Date	e CVSS	C	escriptio	n & CVE I	D	Pato	ch	NCIIP	C ID
				code.							
				CVE	D : CVE	2019-6	334				
pagewide_er	iterp	rise_flo	w_mfp_5	86z_g1	lw40a						
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu		rprise, anged Pri on to che gnature tential orbitrary	nnd nters eck that	N/A		H-HP-PAGE- 051119/224	
					D : CVE	2019-6	334				
pagewide_en	iterp	rise_flo	w_mfp_5	86z_g1	lw41a						
Improper Input Validation	16-	10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.				N/A		H-HP-P. 051119	
					D : CVE-	2019-6	334				
pagewide_en	iterp	rise_mf	p_586_g1	1w39a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have appli may a execu	aserJet, FeJet EnterJet Mana a solution cation si allow po ation of a	rprise, a aged Pri on to che gnature tential orbitrary	nnd nters eck that	N/A		H-HP-P. 051119	
pagewide_er	iterp	rise_mf	p_586_g	lw40a							
Improper Input Validation	16-	10-2019	7.5	Office Laser	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check		H-HP-PAGE- 051119/2246				
CV Scoring Sca (CVSS)	ale	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 signature that may allow potential execution of arbitrary code.		
			CVE ID : CVE-2019-6334		
pagewide_er	nterprise_mfp_	586_g1	w41a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2247
pagewide_m	anaged_flow_n	nfp_e58	B650z_l3u42a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2248
pagewide_m	anaged_flow_n	nfp_e58	B650z_l3u43a		
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-PAGE- 051119/2249
pagewide m	anaged_mfp_e	58650a			
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pul	olish Date	cvss	D	escriptio	n & CVE I	D		Pato	h	NC	IIPC ID
Input Validation				Laser have applie may a execu	Jet Ente Jet Mana a solution cation si allow po ation of a	aged Pri on to che gnature tential arbitrary	nters eck that				0511:	19/2250
pagewide_ma	anag	ed_mfp_	e58650	dn_l3u	43a							
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu- code.	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334			PAGE- 19/2251				
scanjet_enter	pris	e_8500_	fn1_doc	ument	_captur	e_work	station	1_l27	717a			
Improper Input Validation	16-	10-2019	7.5	Office Laser have applie may a execu	Iment_capture_workstation HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code.		N/A	Α			SCAN- 19/2252	
digital_sende	r_flo	w_8500	_fn2_do	cumen	t_captu	re_worl	kstatio	n_l2	762a	ì		
Improper Input Validation		10-2019		HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334				N/A			H-HP- 0511	DIGI- 19/2253
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
scanjet_enter	rprise_flow_n9	120_fn	2_document_scanner_l276	3a	
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. CVE ID: CVE-2019-6334	N/A	H-HP-SCAN- 051119/2254
inea				<u> </u>	
me-rtu					
Incorrect Default Permissions	28-10-2019	4	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A world-readable /usr/smartrtu/init/settin gs.xml configuration file on the file system allows an attacker to read sensitive configuration settings such as usernames, passwords, and other sensitive RTU data due to insecure permission assignment. CVE ID: CVE-2019-14925	N/A	H-INE-ME-R- 051119/2255
Use of Hard- coded Credentials	28-10-2019	7.5	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Hard-coded SSH keys allow an attacker to gain unauthorised access or disclose encrypted data on the RTU	N/A	H-INE-ME-R- 051119/2256
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	Pu	blish Date	cvss	Description & CVE ID				Pa	itch	NCIIP	CID
				regentinstal firmwword private/, /etc/ey, and /etc/y files availate web seconds.	erated of lation of vare upon s, these of te-key versh ssh ssh ssh ssh ssh ssh ssh ssh ssh	lates. In devices in alues in host_rsa host_ec host_ds e publich n the ver	other use a_key dsa_k a_ke y				
Information Exposure	28-	10-2019	5	on Mi RTU of and II throu unaut config vulne attack smart file (v such a passv sensit	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote configuration download vulnerability allows an attacker to download the smartRTU's configuration file (which contains data such as usernames, passwords, and other sensitive RTU data). CVE ID: CVE-2019-					H-INE-N 051119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	28-	10-2019	3.5	An isson Mi RTU of and II throu stored (XSS)	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A number of stored cross-site script (XSS) vulnerabilities allow an attacker to inject			N/A		H-INE-N 051119	
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	Pub	lish Date	cvss	D	escriptio	scription & CVE ID			:h	NCIIP	C ID
				into t exam vulne Serial	ious cod he appli ple inpu rable to IInitialM index.p	cation. A t variabl stored X odemSt	in le KSS is ring				
				CVE I 1492	D : CVE- 8	2019-					
Insufficientl y Protected Credentials	28-1	10-2019	5	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Stored cleartext passwords could allow an unauthenticated attacker to obtain configured username and password combinations on the RTU due to the weak credentials management on the RTU. An unauthenticated user can obtain the exposed password credentials to gain access to the following services: DDNS service, Mobile Network Provider, and OpenVPN service. CVE ID: CVE-2019-14929				N/A		H-INE-N 051119	
Use of Hard- coded Credentials	28-1	10-2019	10	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Undocumented hard-coded user passwords for root, ineaadmin, mitsadmin, and maint				N/A		H-INE-N 051119	
CV Scoring Sca (CVSS)	ile	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 allow an attacker to gain unauthorised access to the RTU. (Also, the accounts ineaadmin and mitsadmin are able to escalate privileges to root without supplying a password due to insecure entries in /etc/sudoers on the RTU.) CVE ID: CVE-2019-14930		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	28-10-2019	10	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote OS Command Injection vulnerability allows an attacker to execute arbitrary commands on the RTU due to the passing of unsafe user supplied data to the RTU's system shell. Functionality in mobile.php provides users with the ability to ping sites or IP addresses via Mobile Connection Test. When the Mobile Connection Test is submitted, action.php is called to execute the test. An attacker can use a shell command separator (;) in the host variable to execute operating system commands upon submitting the test data.	N/A	H-INE-ME-R- 051119/2261

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019- 14931		
mi	,				
millet_route	r_3g				
Improper Input Validation	23-10-2019	7.5	An issue was discovered on Xiaomi Mi WiFi R3G devices before 2.28.23-stable. The backup file is in tar.gz format. After uploading, the application uses the tar zxf command to decompress, so one can control the contents of the files in the decompressed directory. In addition, the application's sh script for testing upload and download speeds reads a URL list from /tmp/speedtest_urls.xml, and there is a command injection vulnerability, as demonstrated by api/xqnetdetect/netspeed. CVE ID: CVE-2019-18370	N/A	H-MI-MILL- 051119/2262
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-10-2019	5	An issue was discovered on Xiaomi Mi WiFi R3G devices before 2.28.23-stable. There is a directory traversal vulnerability to read arbitrary files via a misconfigured NGINX alias, as demonstrated by api-third-party/download/extdisks/etc/config/account. With this vulnerability, the attacker can bypass	N/A	H-MI-MILL- 051119/2263

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			authentication. CVE ID: CVE-2019- 18371		
Mitsubishiel	ectric				
smartrtu					
Incorrect Default Permissions	28-10-2019	4	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A world-readable /usr/smartrtu/init/settin gs.xml configuration file on the file system allows an attacker to read sensitive configuration settings such as usernames, passwords, and other sensitive RTU data due to insecure permission assignment. CVE ID: CVE-2019-14925	N/A	H-MIT-SMAR- 051119/2264
Use of Hard- coded Credentials	28-10-2019	7.5	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Hard-coded SSH keys allow an attacker to gain unauthorised access or disclose encrypted data on the RTU due to the keys not being regenerated on initial installation or with firmware updates. In other words, these devices use private-key values in /etc/ssh/ssh_host_rsa_key	N/A	H-MIT-SMAR- 051119/2265

Weakness	Publish Date	cvss	Description &	CVE ID	Patc	h	NCIIP	C ID
			/etc/ssh/ssh_ho ey, and /etc/ssh/ssh_ho y files that are pravailable from the web sites. CVE ID : CVE-20	ost_dsa_ke ublicly he vendor				
Information Exposure	28-10-2019	5	An issue was disson Mitsubishi El RTU devices throad INEA ME-RT through 3.0. An unauthenticated configuration do vulnerability alloattacker to down smartRTU's confile (which contasuch as usernam passwords, and sensitive RTU da CVE ID: CVE-20 14927	ectric ME- ough 2.02 I'U devices I remote ownload ows an nload the figuration ains data nes, other ata).	N/A		H-MIT-9 051119	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	28-10-2019	3.5	An issue was dison Mitsubishi El RTU devices through 3.0. A not stored cross-site (XSS) vulnerabilian attacker to in malicious code of into the applicate example input vulnerable to sto SerialInitialMod in the index.php	ectric ME- ough 2.02 FU devices umber of e script lities allow ject directly cion. An ariable ored XSS is emString page.	N/A		H-MIT-9 051119	
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
			14928		
Insufficientl y Protected Credentials	28-10-2019	5	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Stored cleartext passwords could allow an unauthenticated attacker to obtain configured username and password combinations on the RTU due to the weak credentials management on the RTU. An unauthenticated user can obtain the exposed password credentials to gain access to the following services: DDNS service, Mobile Network Provider, and OpenVPN service. CVE ID: CVE-2019-14929	N/A	H-MIT-SMAR- 051119/2268
Use of Hard- coded Credentials	28-10-2019	10	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Undocumented hard-coded user passwords for root, ineaadmin, mitsadmin, and maint could allow an attacker to gain unauthorised access to the RTU. (Also, the accounts ineaadmin and mitsadmin are able to escalate privileges to root without supplying a	N/A	H-MIT-SMAR- 051119/2269

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
			password due to insecure entries in /etc/sudoers on the RTU.)				
			CVE ID : CVE-2019- 14930				
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	28-10-2019	10	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote OS Command Injection vulnerability allows an attacker to execute arbitrary commands on the RTU due to the passing of unsafe user supplied data to the RTU's system shell. Functionality in mobile.php provides users with the ability to ping sites or IP addresses via Mobile Connection Test. When the Mobile Connection Test is submitted, action.php is called to execute the test. An attacker can use a shell command separator (;) in the host variable to execute operating system commands upon submitting the test data. CVE ID: CVE-2019-14931	N/A	H-MIT-SMAR- 051119/2270		
Ricoh mp_501							
Improper Neutralizati	21-10-2019	4.3	On the RICOH MP 501 printer, HTML Injection N/A H-RIC-MP_5 051119/222				
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	D	escription	& CVE II	D	Pato	:h	NCIIP	CID
on of Input During Web Page Generation ('Cross-site Scripting')			and Stored XSS vulnerabilities have been discovered in the area of adding addresses via the entryNameIn and KeyDisplay parameter to /web/entry/en/address/a drsSetUserWizard.cgi. CVE ID: CVE-2019- 18203							
Samsung										
galaxy_s10										
Improper Input Validation	17-10-2019	4.4	Note1 unloc unreg in cer involv scree	Samsung Galaxy S10 and Note10 devices allow unlock operations via unregistered fingerprints in certain situations involving a third-party screen protector. CVE ID: CVE-2019- 17668		N/A		H-SAM- 051119		
note_10										
Improper Input Validation	17-10-2019	4.4	Note1 unloc unreg in cer involv scree	Samsung Galaxy S10 and Note10 devices allow unlock operations via unregistered fingerprints in certain situations involving a third-party screen protector.		N/A		H-SAM- 051119		
			CVE ID : CVE-2019- 17668							
Sangoma							<u> </u>			
session_bord	ler_controller									
Improper Neutralizati on of Special Elements in Output Used	22-10-2019	5	The Sangoma Session Border Controller (SBC) 2.3.23-119 GA web interface is vulnerable to Argument Injection via			N/A		H-SAN- 051119		
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
by a Downstrea m Component ('Injection')			special characters in the username field. Upon successful exploitation, a remote unauthenticated user can create a local system user with sudo privileges, and use that user to login to the system (either via the web interface or via SSH) to achieve complete compromise of the device. This affects /var/webconfig/gui/Webc onfig.inc.php and /usr/local/sng/bin/sng-user-mgmt. CVE ID: CVE-2019-12147		
Improper Authenticati on	22-10-2019	7.5	The Sangoma Session Border Controller (SBC) 2.3.23-119 GA web interface is vulnerable to an authentication bypass via an argument injection vulnerability involving special characters in the username field. Upon successful exploitation, a remote unauthenticated user can login into the device's admin web portal without providing any credentials. This affects /var/webconfig/gui/Webc onfig.inc.php. CVE ID: CVE-2019- 12148	N/A	H-SAN-SESS- 051119/2275
terra-master					

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D		Pato	:h	NCIIP	CID
f2-210											
Improper Privilege Managemen t	28-10-2019	6.5	on Te 4.0.19 users for pr	erraMast O device can use rivilege of D: CVE	discover er FS-21 s. Norma 1.user.p elevatior	l0 al ohp	N/	'A		H-TER- 051119	
fs-210											
Information Exposure Through Log Files	23-10-2019	on TerraMaster FS-210 4.0.19 devices. An unauthenticated attacker can download log files via the include/makecvs.php?Eve nt= substring. CVE ID: CVE-2019-				4.0.19 devices. An unauthenticated attacker can download log files via the include/makecvs.php?Eve nt= substring.				H-TER- 051119	
Tp-link											
m7350											
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-10-2019	10	throu 1812 exter Inject	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow externalPort OS Command Injection (issue 1 of 5). CVE ID: CVE-2019-13649		N/A			H-TPM73 051119/22		
Improper Neutralizati on of Special Elements used in an OS Command	24-10-2019	10	throu 1812 interi Inject	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow internalPort OS Command Injection (issue 2 of 5). CVE ID: CVE-2019- 13650			N/	'A		H-TPN 051119	
CV Scoring Sca (CVSS)	o-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	
('OS Command Injection')						
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow portMappingProtocol OS Command Injection (issue 3 of 5). CVE ID: CVE-2019-13651	N/A	H-TPM735- 051119/2280	
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow serviceName OS Command Injection (issue 4 of 5). CVE ID: CVE-2019-13652	N/A	H-TPM735- 051119/2281	
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	24-10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow triggerPort OS Command Injection (issue 5 of 5). CVE ID: CVE-2019-13653	N/A	H-TPM735- 051119/2282	
Wago						
pfc200						
Externally Controlled Reference to a Resource	19-10-2019	5	Information Disclosure is possible on WAGO Series PFC100 and PFC200 devices before FW12 due	N/A	H-WAG-PFC2- 051119/2283	
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
in Another Sphere			to improper access control. A remote attacker can check for the existence of paths and file names via crafted HTTP requests.		
pfc100			CVE ID : CVE-2019- 18202		
picioo			Information Disclosure is		
Externally Controlled Reference to a Resource in Another Sphere	19-10-2019	5	possible on WAGO Series PFC100 and PFC200 devices before FW12 due to improper access control. A remote attacker can check for the existence of paths and file names via crafted HTTP requests. CVE ID: CVE-2019- 18202	N/A	H-WAG-PFC1- 051119/2284