Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Adobe					
experience_manager					
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/security/products/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/security/products/experience-manager/aps b19-48.html	A-ADO-EXPE-041119/2
Improper Neutralization of Special Elements in Output Used by a Downstream 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/security/products/experience-manager/aps b19-48.html	A-ADO-EXPE-041119/3
Improper Neutralization 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/security/produc	A-ADO-EXPE-041119/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2019-8078**	ts/experience-manager/apsb19-48.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	4.3	Adobe Experience Manager versions 6.4, 6.3, 6.2, 6.1, and 6.0 have a stored cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2019-8079**	https://helpx.adobe.com/security/products/experience-manager/apsb19-48.html	A-ADO-EXPE-041119/5
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	4.3	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**	https://helpx.adobe.com/security/products/experience-manager/apsb19-48.html	A-ADO-EXPE-041119/6
Improper Authentication	25-10-2019	5	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**	https://helpx.adobe.com/security/products/experience-manager/apsb19-48.html	A-ADO-EXPE-041119/7
Improper Restriction of XML External Entity Reference	25-10-2019	5	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://helpx.adobe.com/security/products/experience-manager/aps	A-ADO-EXPE-041119/8

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
('XXE')			disclosure. **CVE ID : CVE-2019-8082**	b19-48.html	
Improper Neutralization 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/security/products/experience-manager/apsb19-48.html	A-ADO-EXPE-041119/9
Improper Neutralization 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/security/products/experience-manager/apsb19-48.html	A-ADO-EXPE-041119/10
Improper Neutralization 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/security/products/experience-manager/apsb19-48.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/security/products/experience-manager/apsb19-48.html	A-ADO-EXPE-041119/12
download_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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/security/products/adm/apsb19-51.html	A-ADO-DOWN-041119/13
acrobat_dc					
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/14
Improper Neutralization 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 disclosure. **CVE ID : CVE-2019-8160**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/15
Incorrect	17-10-2019	7.5	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-

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/security/products/acrobat/apsb19-49.html	041119/16
Concurrent Execution using Shared Resource with Improper Synchronization ('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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/18

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
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/19
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/20
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/21

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
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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8168		
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/24
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 . **CVE ID : CVE-2019-8170**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/25
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/26

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
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/27
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/28
NULL Pointer Dereference	17-10-2019	6.8	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier,	https://helpx.adobe.com/security/produc	A-ADO-ACRO-041119/29

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
			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**	ts/acrobat/apsb19-49.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-2019-8175**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/30
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/31

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 . **CVE ID : CVE-2019-8177**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/33
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/34

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-2019-8179**		
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/35
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-2019-8181**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/36
Out-of-	17-10-2019	5	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/39

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
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/40
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/41
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/42

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
			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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8189		
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/45
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-2019-8191**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/46
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/47

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
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/48
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/49
NULL Pointer Dereference	17-10-2019	10	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier,	https://helpx.adobe.com/security/produc	A-ADO-ACRO-041119/50

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 untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-8195**	ts/acrobat/apsb19-49.html	
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 . **CVE ID : CVE-2019-8196**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/51
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/52

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

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, 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/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/54
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/55

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/57
Use After	17-10-2019	6.8	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-

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-2019-8203**	adobe.com/security/products/acrobat/apsb19-49.html	041119/58
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 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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/59
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to 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 . **CVE ID : CVE-2019-8206**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/61
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/62
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/63

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8210		
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/66
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-2019-8212**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/67
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/68

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-2019-8213**		
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 . **CVE ID : CVE-2019-8214**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/69
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-2019-8215**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/70
Out-of-bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier,	https://helpx.adobe.com/security/produc	A-ADO-ACRO-041119/71

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 read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-8216**	ts/acrobat/apsb19-49.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-2019-8217**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/72
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/73

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
			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/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/76

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-2019-8221**		
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/77
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/78
Use After	17-10-2019	6.8	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-

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-2019-8224**	adobe.com/security/products/acrobat/apsb19-49.html	041119/79
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-2019-8225**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/80
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/81

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
			security mechanism vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-8226**		
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. **CVE ID : CVE-2019-8237**	N/A	A-ADO-ACRO-041119/82
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-ACRO-041119/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. **CVE ID : CVE-2019-8238**		
acrobat_reader_dc					
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/84
Improper Neutralization 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 disclosure. **CVE ID : CVE-2019-8160**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/85
Incorrect Type	17-10-2019	7.5	Adobe Acrobat and Reader versions , 2019.012.20040	https://helpx.adobe.com/se	A-ADO-ACRO-041119/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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/products/acrobat/apsb19-49.html	
Concurrent Execution using Shared Resource with Improper Synchronization ('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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/87
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/88

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
			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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/94
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 . **CVE ID : CVE-2019-8170**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/95
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-	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/96

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/ap	A-ADO-ACRO-041119/99

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 . **CVE ID : CVE-2019-8175**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/102
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/103
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/104

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-2019-8179**		
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/105
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-2019-8181**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/106
Out-of-bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier,	https://helpx.adobe.com/security/produc	A-ADO-ACRO-041119/107

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 read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-8182**	ts/acrobat/apsb19-49.html	
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/108
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/109

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

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 . **CVE ID : CVE-2019-8185**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/112

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. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-8188**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/113
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/114
Out-of-	17-10-2019	4.3	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-

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/security/products/acrobat/apsb19-49.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/117

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
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/118
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/119
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/120

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 . **CVE ID : CVE-2019-8196**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/123
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/124
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/125

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
			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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/produc	A-ADO-ACRO-041119/128

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-2019-8203**	ts/acrobat/apsb19-49.html	
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 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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/129
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/130

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 . **CVE ID : CVE-2019-8206**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/133

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-2019-8208**		
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/134
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-2019-8210**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/135
Use After	17-10-2019	7.5	Adobe Acrobat and Reader	https://helpx.	A-ADO-ACRO-

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-2019-8211**	adobe.com/security/products/acrobat/apsb19-49.html	041119/136
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-2019-8212**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/137
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.	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/138

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
			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 . **CVE ID : CVE-2019-8214**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/139
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-2019-8215**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/140
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/141

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

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/144
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/145
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/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/146

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/produc	A-ADO-ACRO-041119/149

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-2019-8224**	ts/acrobat/apsb19-49.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-2019-8225**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/150
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 security mechanism vulnerability. Successful	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	A-ADO-ACRO-041119/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to information disclosure. **CVE ID : CVE-2019-8226**		
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. **CVE ID : CVE-2019-8237**	N/A	A-ADO-ACRO-041119/152
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	N/A	A-ADO-ACRO-041119/153

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_cloud					
Improper Privilege Management	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_manager_forms					
Improper Neutralization 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/security/products/aem-forms/apsb19-50.html	A-ADO-EXPE-041119/155
ant.design					
ant_design_pro					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Apache					
traffic_server					
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-TRAF-041119/157
thrift					
Loop with Unreachable Exit Condition ('Infinite Loop')	29-10-2019	7.8	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. **CVE ID : CVE-2019-0205**	N/A	A-APA-THRI-041119/158
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://mail-archives.apache.org/mod_mbox/thrift-dev/201910.mbox/%3C277A46CA87494176B1BBCF5D72624A2A	A-APA-THRI-041119/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				%40HAGGIS%3E	
poi					
Improper Restriction of XML External Entity Reference ('XXE')	23-10-2019	2.1	In Apache POI up to 4.1.0, when using the tool XSSFExportToXml to convert user-provided Microsoft Excel documents, a specially crafted document can allow an attacker to read files from the local filesystem or from internal network resources via XML External Entity (XXE) Processing. **CVE ID : CVE-2019-12415**	N/A	A-APA-POI-041119/160
Avast					
antivirus					
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\wbemcomn.dll, which is loaded into a protected-light 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.	N/A	A-AVA-ANTI-041119/161

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
			CVE ID : CVE-2019-17093		
AVG					
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\wbemcomn.dll, which is loaded into a protected-light 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					
network_operations					
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://techdocs.broadcom.com/us/product-content/recommended-reading/security-notices/ca-20191015-01-security-notice-for-ca-	A-BRO-NETW-041119/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13657	performance-management.html	
ca_performance_management					
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://techdocs.broadcom.com/us/product-content/recommended-reading/security-notices/ca-20191015-01-security-notice-for-ca-performance-management.html	A-BRO-CA_P-041119/164
Cisco					
wireless_lan_controller_software					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-10-2019	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to view system files that may contain sensitive information. **CVE ID : CVE-2019-15266**		
firepower_management_center					
Improper Neutralization 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) Software could allow an authenticated, remote attacker to conduct a stored 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 inserting malicious code in certain sections of the interface that are visible to other users. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. An attacker would need valid administrator credentials to exploit this vulnerability.	N/A	A-CIS-FIRE-041119/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15280		
identity_services_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web-based management interface. The vulnerabilities are due to insufficient validation of user-supplied input that is processed 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-2019-12637**	N/A	A-CIS-IDEN-041119/167
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-10-2019	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-IDEN-041119/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			site scripting (XSS) attacks against a user of the web-based management interface. The vulnerability is due to insufficient validation of user-supplied input that is processed 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-2019-12638**		
telepresence_video_communication_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	A vulnerability in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. The vulnerability is due to insufficient validation of user-supplied	N/A	A-CIS-TELE-041119/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input by the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious 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-2019-12705**		
telepresence_collaboration_endpoint					
Improper Privilege Management	16-10-2019	6.6	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 filesystem. The attacker	N/A	A-CIS-TELE-041119/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has no control over the contents of the data written to the file. Overwriting a critical file could cause the device to crash, resulting in a denial of service condition (DoS). **CVE ID : CVE-2019-15273**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-10-2019	7.2	A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to perform command injections. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating as an administrative level user within the restricted shell and submitting malicious input to a specific command. A successful exploit could allow the attacker to execute previously staged code from the underlying filesystem. **CVE ID : CVE-2019-15274**	N/A	A-CIS-TELE-041119/171
Improper Privilege Management	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-TELE-041119/172

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 Management	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 Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			root privileges. **CVE ID : CVE-2019-15277**		
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	A-CIS-TELE-041119/174
identity_services_engine_software					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The attacker must have valid administrator credentials. The vulnerability is due to insufficient validation of user-supplied input by the	N/A	A-CIS-IDEN-041119/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management 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, browser-based information. **CVE ID : CVE-2019-15281**		
Missing Authenticati on for Critical Function	16-10-2019	5	A vulnerability in the web-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-2019-15282**	N/A	A-CIS-IDEN-041119/176

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
Cmsmadesimple					
cms_made_simple					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	CMS Made Simple (CMSMS) 2.2.11 allows stored XSS by an admin via a crafted image filename on the "file manager > upload images" screen. **CVE ID : CVE-2019-17629**	N/A	A-CMS-CMS_-041119/177
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	CMS Made Simple (CMSMS) 2.2.11 allows stored XSS by an admin via a crafted image filename on the "News > Add Article" screen. **CVE ID : CVE-2019-17630**	N/A	A-CMS-CMS_-041119/178
Codesys					
eni_server					
Out-of-bounds Write	25-10-2019	7.5	CODESYS V2.3 ENI server up to V3.2.2.24 has a Buffer Overflow. **CVE ID : CVE-2019-16265**	https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-09_LCDS-319.pdf	A-COD-ENI_-041119/179
codesys					
Out-of-bounds Write	25-10-2019	7.5	CODESYS V2.3 ENI server up to V3.2.2.24 has a Buffer Overflow. **CVE ID : CVE-2019-16265**	https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-09_LCDS-	A-COD-CODE-041119/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				319.pdf	
corehr					
core_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-10-2019	4.3	CoreHR Core Portal before 27.0.7 allows stored XSS. **CVE ID : CVE-2019-18221**	N/A	A-COR-CORE-041119/181
Craftcms					
craft_cms					
Weak Password Recovery Mechanism for Forgotten Password	24-10-2019	5	In Craft CMS through 3.1.7, the elevated session password prompt was not being rate limited like normal login forms, leading to the possibility of a brute force attempt on them. **CVE ID : CVE-2019-15929**	N/A	A-CRA-CRAF-041119/182
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-THIN-041119/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			../../ThinVnc.ini directory traversal attack vector. **CVE ID : CVE-2019-17662**		
darktrace					
enterprise_immune_system					
Cross-Site Request Forgery (CSRF)	23-10-2019	4.3	Darktrace Enterprise Immune System before 3.1 allows CSRF via the /whitelisteddomains endpoint. **CVE ID : CVE-2019-9596**	N/A	A-DAR-ENTE-041119/184
Cross-Site Request Forgery (CSRF)	23-10-2019	4.3	Darktrace Enterprise Immune System before 3.1 allows CSRF via the /config endpoint. **CVE ID : CVE-2019-9597**	N/A	A-DAR-ENTE-041119/185
dkd					
direct_mail					
Information Exposure	16-10-2019	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. **CVE ID : CVE-2019-16698**	https://typo3.org/security/advisory/typo3-ext-sa-2019-016/	A-DKD-DIRE-041119/186
doas_project					
doas					
N/A	18-10-2019	10	An issue was discovered in slicer69 doas before 6.2 on certain platforms other	N/A	A-DOA-DOAS-041119/187

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					
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			via the "outgoing email setup" feature in the /admin/mails.php?action=edit URI via the "Send all emails to (instead of real recipients, for test purposes)" field. **CVE ID : CVE-2019-17576**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	An issue was discovered in Dolibarr 10.0.2. It has XSS via the "outgoing email setup" feature in the admin/mails.php?action=edit URI via the "Email used for error returns emails (fields 'Errors-To' in emails sent)" field. **CVE ID : CVE-2019-17577**	N/A	A-DOL-DOLI-041119/190
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	An issue was discovered in Dolibarr 10.0.2. It has XSS via the "outgoing email setup" feature in the admin/mails.php?action=edit URI via the "Sender email for automatic emails (default value in php.ini: Undefined)" field. **CVE ID : CVE-2019-17578**	N/A	A-DOL-DOLI-041119/191
dormsystem_project					
dormsystem					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Eclipse					
openj9					
Incorrect Permission Assignment for Critical Resource	17-10-2019	6.4	From Eclipse OpenJ9 0.15 to 0.16, access to diagnostic operations such as causing a GC or creating a diagnostic file are permitted without any privilege checks. **CVE ID : CVE-2019-17631**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=552129	A-ECL-OPEN-041119/193
wild_web_developer					
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-2019-18212**	https://github.com/angelozerr/lsp4xml/blob/master/CHANGELOG.md#others	A-ECL-WILD-041119/194
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://github.com/angelozerr/lsp4xml/blob/master/CHANGELOG.md#others	A-ECL-WILD-041119/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			challenge/response capture for password cracking). This occurs in extensions/contentmodel/participants/diagnostics/LSPXMLParserConfiguration.java. **CVE ID : CVE-2019-18213**		
eq-3					
cux-daemon					
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	A-EQ--CUX--041119/196
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. **CVE ID : CVE-2019-14424**	N/A	A-EQ--CUX--041119/197
etherpad					
etherpad					
Improper Neutralizati	19-10-2019	4.3	templates/pad.html in Etherpad-Lite 1.7.5 has	N/A	A-ETH-ETHE-041119/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			XSS when the browser does not encode the path of the URL, as demonstrated by Internet Explorer. **CVE ID : CVE-2019-18209**		
eu_cookie_law_project					
eu_cookie_law					
Improper Neutralization 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-EU_-EU_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18218		
forcepoint					
one_endpoint					
Incorrect Authorization	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-ONE_-041119/201
Fortinet					
forticlient					
Uncontrolled 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-FORT-041119/202
Foxitsoftware					
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-FOXI-041119/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EPS. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8809. **CVE ID : CVE-2019-17138**		
foxit_reader					
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 to execute code in the context of the current process. Was ZDI-CAN-	N/A	A-FOX-FOXI-041119/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8692. **CVE ID : CVE-2019-17139**		
phantompdf					
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 to execute code in the context of the current process. Was ZDI-CAN-8692. **CVE ID : CVE-2019-17139**	N/A	A-FOX-PHAN-041119/205
Use After Free	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	N/A	A-FOX-PHAN-041119/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the OnFocus event. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9091. **CVE ID : CVE-2019-17140**		
Use After Free	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 processing of script within a Calculate action of a text field. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current	N/A	A-FOX-PHAN-041119/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process. Was ZDI-CAN-9044. **CVE ID : CVE-2019-17141**		
Use After Free	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 processing of script within a Keystroke action of a listbox field. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9081. **CVE ID : CVE-2019-17142**	N/A	A-FOX-PHAN-041119/208
Use After Free	25-10-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the	N/A	A-FOX-PHAN-041119/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9273. **CVE ID : CVE-2019-17143**		
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 DWG files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current	N/A	A-FOX-PHAN-041119/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-FOX-PHAN-041119/211
Freepbx					
contactmanager					
Improper Neutralization 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-CONT-041119/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			(html\admin\modules\contactmanager\Contactmanager.class.php), an unsanitized group variable coming from the URL is reflected in HTML on 2 occasions, leading to XSS. It can be requested via a GET request to /admin/ajax.php?module=contactmanager. **CVE ID : CVE-2019-16966**		
freepbx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	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 (html\admin\modules\contactmanager\Contactmanager.class.php), an unsanitized group variable coming from the URL is reflected in HTML on 2 occasions, leading to XSS. It can be requested via a GET request to /admin/ajax.php?module=contactmanager. **CVE ID : CVE-2019-16966**	N/A	A-FRE-FREE-041119/213
Improper Neutralization of Input During Web Page Generation	21-10-2019	4.3	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	N/A	A-FRE-FREE-041119/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			(html\admin\modules\manager\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&display=manager. **CVE ID : CVE-2019-16967**		
manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	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 (html\admin\modules\manager\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&display=manager. **CVE ID : CVE-2019-16967**	N/A	A-FRE-MANA-041119/215
fusionpbx					
fusionpbx					
Improper Neutralization 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-FUSI-041119/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Downstream 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 Neutralization of Special Elements in Output Used by a Downstream 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 Neutralization 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-2019-16968**	N/A	A-FUS-FUSI-041119/218
Improper Neutralization of Input During Web Page	21-10-2019	4.3	In FusionPBX up to 4.5.7, the file app\fifo_list\fifo_interactive.php uses an unsanitized "c" variable coming from	N/A	A-FUS-FUSI-041119/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			the URL, which is reflected in HTML, leading to XSS. **CVE ID : CVE-2019-16969**		
Improper Neutralization 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**	N/A	A-FUS-FUSI-041119/220
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-10-2019	4.3	In FusionPBX up to 4.5.7, the file app\messages\messages_thread.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-2019-16971**	N/A	A-FUS-FUSI-041119/221
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-10-2019	4.3	In FusionPBX up to 4.5.7, the file app\contacts\contact_addresses.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-FUSI-041119/222
Improper Neutralization 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-FUSI-041119/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			"query_string" variable coming from the URL, which is reflected in HTML, leading to XSS. **CVE ID : CVE-2019-16973**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	In FusionPBX up to 4.5.7, the file app\contacts\contact_times.php uses an unsanitized "id" variable coming from the URL, which is reflected in HTML, leading to XSS. **CVE ID : CVE-2019-16974**	N/A	A-FUS-FUSI-041119/224
Improper Neutralization 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_notes.php uses an unsanitized "id" variable coming from the URL, which is reflected in HTML, leading to XSS. **CVE ID : CVE-2019-16975**	N/A	A-FUS-FUSI-041119/225
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	In FusionPBX up to 4.5.7, the file app\destinations\destination_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-FUSI-041119/226
Improper Neutralization of Input During Web	23-10-2019	4.3	In FusionPBX up to 4.5.7, the file app\extensions\extension_imports.php uses an	N/A	A-FUS-FUSI-041119/227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			unsanitized "query_string" variable coming from the URL, which is reflected in HTML, leading to XSS. **CVE ID : CVE-2019-16977**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\devices\device_settings.php uses an unsanitized "id" variable coming from the URL, which is reflected on 2 occasions in HTML, leading to XSS. **CVE ID : CVE-2019-16978**	N/A	A-FUS-FUSI-041119/228
Improper Neutralization 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_urls.php uses an unsanitized "id" variable coming from the URL, which is reflected in HTML, leading to XSS. **CVE ID : CVE-2019-16979**	N/A	A-FUS-FUSI-041119/229
Improper Neutralization 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_broadcast_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-FUSI-041119/230
Improper Neutralization of Input	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\conference_profiles\c	N/A	A-FUS-FUSI-041119/231

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 Neutralization 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\access_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 Neutralization 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 Neutralization 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	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML, leading to XSS. **CVE ID : CVE-2019-16984**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-10-2019	8.5	In FusionPBX up to v4.5.7, the file app\xml_cdr\xml_cdr_delete.php uses an unsanitized "rec" variable coming from the URL, which is base64 decoded and allows deletion of any file of the system. **CVE ID : CVE-2019-16985**	N/A	A-FUS-FUSI-041119/235
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-10-2019	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_download.php is also affected.) **CVE ID : CVE-2019-16986**	N/A	A-FUS-FUSI-041119/236
Improper Neutralization 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_import.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-FUSI-041119/237
Improper Neutralization of Input	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\basic_operator_panel	N/A	A-FUS-FUSI-041119/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			\resources\content.php uses an unsanitized "eavesdrop_dest" variable coming from the URL, which is reflected on 3 occasions in HTML, leading to XSS. **CVE ID : CVE-2019-16988**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	In FusionPBX up to v4.5.7, the file app\conferences_active\conference_interactive.php uses an unsanitized "c" variable coming from the URL, which is reflected in HTML, leading to XSS. **CVE ID : CVE-2019-16989**	N/A	A-FUS-FUSI-041119/239
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-10-2019	4	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-2019-16990**	N/A	A-FUS-FUSI-041119/240
Improper Neutralization 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-FUSI-041119/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
GNU					
guix					
Incorrect Permission Assignment for Critical Resource	17-10-2019	4.6	GNU Guix 1.0.1 allows local users to gain access to an arbitrary user's account because the parent directory of the user-profile directories is world writable, a similar issue to CVE-2019-17365. **CVE ID : CVE-2019-18192**	N/A	A-GNU-GUIX-041119/242
libidn2					
Improper Input Validation	22-10-2019	5	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. **CVE ID : CVE-2019-12290**	https://gitlab.com/libidn/libidn2/commit/614117ef6e4c60e1950d742e3edf0a0ef8d389de	A-GNU-LIBI-041119/243
Out-of-bounds Write	21-10-2019	7.5	idn2_to_ascii_4i in lib/lookup.c in GNU libidn2 before 2.1.1 has a	N/A	A-GNU-LIBI-041119/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			heap-based buffer overflow via a long domain string. **CVE ID : CVE-2019-18224**		
goharbor					
harbor					
Incorrect Default Permissions	18-10-2019	5	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 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**	http://www.vmware.com/security/advisories/VMSA-2019-0016.html	A-GOH-HARB-041119/245
Golang					
go					
Interpretation 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://github.com/golang/go/issues/34960, https://groups.google.com/d/msg/golang-announce/lVEm7llp0w0/Vb	A-GOL-GO-041119/246

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 transfer-encoding 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 Neutralization 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://hclpnpsupport.hcltech.com/csm?id=kb_article&sysparm_article=KB0073231	A-HCL-TRAV-041119/248

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 Neutralization 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/advisories/1211	A-HEX-HEXO-041119/249
hongcms_project					
hongcms					
Improper Neutralization 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 Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Improper Neutralization 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 Neutralization 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 Neutralization 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 Neutralization 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=update_f&user_name= or admin/user.php?form=remove_f&user_name= or admin/config/diff.php?app= URI, related to the Tag Cloud feature. **CVE ID : CVE-2019-**	N/A	A-HOR-GROU-041119/255

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. **CVE ID : CVE-2019-12095**	N/A	A-HOR-GROU-041119/256
hornerautomation					
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_lodge_management_system_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hotel_and_lodge_management_system					
Improper Neutralization 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-2019-18387**	N/A	A-HOT-HOTE-041119/259
IBM					
security_guardium_big_data_intelligence					
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. **CVE ID : CVE-2019-4306**	https://www.ibm.com/support/pages/node/1096396	A-IBM-SECU-041119/260
Insufficiently 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/support/pages/node/1096288	A-IBM-SECU-041119/261
Use of Hard-	29-10-2019	2.1	IBM Security Guardium	https://www.	A-IBM-SECU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			Big Data Intelligence (SonarG) 4.0 uses hard coded credentials which could allow a local user to obtain highly sensitive information. IBM X-Force ID: 161035. **CVE ID : CVE-2019-4309**	ibm.com/support/pages/node/1096348	041119/262
Information Exposure	29-10-2019	5	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161037. **CVE ID : CVE-2019-4311**	https://www.ibm.com/support/pages/node/1098069	A-IBM-SECU-041119/263
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://www.ibm.com/support/pages/node/1096912	A-IBM-SECU-041119/264
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/support/pages/node/1096906	A-IBM-SECU-041119/265

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
Reliance on Cookies without Validation and Integrity Checking	29-10-2019	4.3	IBM Security Guardium 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**	https://www.ibm.com/support/pages/node/1096384	A-IBM-SECU-041119/266
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 attacker to decrypt highly sensitive information. IBM X-Force ID: 161418. **CVE ID : CVE-2019-4339**	https://www.ibm.com/support/pages/node/1096924	A-IBM-SECU-041119/267
cloud_orchestrator					
Improper Input Validation	25-10-2019	2.1	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 contain APIs that could be used by a local user to send email. IBM X-Force ID: 162232. **CVE ID : CVE-2019-4394**	https://www.ibm.com/support/pages/node/1097301	A-IBM-CLOU-041119/268
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/support/pages/node/1097175	A-IBM-CLOU-041119/269
Improper	25-10-2019	3.5	IBM Cloud Orchestrator	https://www.	A-IBM-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			2.4 through 2.4.0.5 and 2.5 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.com/support/pages/node/1096354	041119/270
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 **CVE ID : CVE-2019-4397**	https://www.ibm.com/support/pages/node/1077147	A-IBM-CLOU-041119/271
Missing Encryption of Sensitive	24-10-2019	2.1	IBM Cloud Orchestrator and IBM Cloud Orchestrator Enterprise	https://www.ibm.com/support/pages/n	A-IBM-CLOU-041119/272

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 Cryptographic 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/support/pages/node/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/support/pages/node/1077129	A-IBM-CLOU-041119/274
Improper Neutralization 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/support/pages/node/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/support/pages/node/1072684	A-IBM-CLOU-041119/276
cloud_orchestrator_enterprise					
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/support/pages/node/1077147	A-IBM-CLOU-041119/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4397		
Missing Encryption of Sensitive Data	24-10-2019	2.1	IBM Cloud Orchestrator and IBM Cloud Orchestrator Enterprise 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**	https://www.ibm.com/support/pages/node/1077123	A-IBM-CLOU-041119/278
db2_high_performance_unload_load					
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. **CVE ID : CVE-2019-4523**	https://supportcontent.ibm.com/support/pages/node/1073236	A-IBM-DB2_-041119/279
maximo_health\,_safety_and_environment_manager					
Improper Privilege Management	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/support/pages/node/1087738	A-IBM-MAXI-041119/280
api_connect					
Information	29-10-2019	5	IBM API Connect version	https://www.	A-IBM-API_-

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. **CVE ID : CVE-2019-4600**	ibm.com/support/pages/node/1079127	041119/281
maximo_asset_management					
Improper Neutralization 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 Neutralization 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-041119/283
maximo_for_life_sciences					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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-041119/284
maximo_for_nuclear_power					
Improper Neutralization 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-041119/285
maximo_for_oil_and_gas					
Improper Privilege Management	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/support/pages/node/1087738	A-IBM-MAXI-041119/286

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
Improper Neutralization 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					
Improper Neutralization 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-041119/288
maximo_for_utilities					
Improper Neutralization 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/support/pages/node/1075023	A-IBM-MAXI-041119/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 164070. **CVE ID : CVE-2019-4486**		
smartcloud_control_desk					
Improper Neutralization 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-SMAR-041119/290
tivoli_integration_composer					
Improper Neutralization 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-TIVO-041119/291
tivoli_workload_scheduler					
Improper Privilege	16-10-2019	7.2	IBM Workload Scheduler Distributed 9.2, 9.3, 9.4,	https://www.ibm.com/sup	A-IBM-TIVO-041119/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			and 9.5 contains a vulnerability that could allow a local user to write files as root in the file system, which could allow the attacker to gain root privileges. IBM X-Force ID: 155997. **CVE ID : CVE-2019-4031**	port/pages/node/1076775	
security_access_manager					
Improper Input Validation	25-10-2019	5	IBM Security Access Manager Appliance could allow unauthenticated attacker to cause a denial of service in the reverse proxy component. IBM X-Force ID: 156159. **CVE ID : CVE-2019-4036**	https://www.ibm.com/support/pages/node/1072704	A-IBM-SECU-041119/293
ics					
kea					
Reachable Assertion	16-10-2019	3.3	A packet containing a malformed DUID can cause the Kea DHCPv6 server process (kea-dhcp6) 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://kb.isc.org/docs/cve-2019-6472	A-ICS-KEA-041119/294
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://kb.isc.org/docs/cve-2019-6473	A-ICS-KEA-041119/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.6.0-beta2. **CVE ID : CVE-2019-6473**		
Igniterealtime					
openfire					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-10-2019	5	PluginServlet.java in Ignite Realtime Openfire through 4.4.2 does not ensure that retrieved files are located under the Openfire home directory, aka a directory traversal vulnerability. **CVE ID : CVE-2019-18393**	N/A	A-IGN-OPEN-041119/296
Server-Side Request Forgery (SSRF)	24-10-2019	7.5	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-OPEN-041119/297
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://kb.isc.org/docs/cve-2019-6474	A-ISC-KEA-041119/298

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					
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://security.netapp.com/advisory/ntap-20191024-0004/	A-ISC-BIND-041119/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			recursive server using a mirror zone and a root name server, this vulnerability could then be used to cause the recursive server to accept a copy of falsified root zone data. This affects BIND versions 9.14.0 up to 9.14.6, and 9.15.0 up to 9.15.4. **CVE ID : CVE-2019-6475**		
Reachable Assertion	17-10-2019	5	A defect in code added to support QNAME minimization can cause named to exit with an assertion failure if a forwarder returns a referral rather than resolving the query. This affects BIND versions 9.14.0 up to 9.14.6, and 9.15.0 up to 9.15.4. **CVE ID : CVE-2019-6476**	https://kb.isc.org/docs/cve-2019-6476, https://security.netapp.com/advisory/ntap-20191024-0004/	A-ISC-BIND-041119/300
Jenkins					
bumblebee_hp_alm					
Improper Certificate Validation	16-10-2019	6.4	Jenkins Bumblebee HP ALM Plugin 4.1.3 and earlier unconditionally disabled SSL/TLS and hostname verification for connections to HP ALM. **CVE ID : CVE-2019-10444**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1481	A-JEN-BUMB-041119/301
google_kubernetes_engine					
Incorrect Permission Assignment	16-10-2019	4	A missing permission check in Jenkins Google Kubernetes Engine Plugin	https://jenkins.io/security/advisory/201	A-JEN-GOOG-041119/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
for Critical Resource			0.7.0 and earlier allowed attackers with Overall/Read permission to obtain limited information about the scope of a credential with an attacker-specified credentials ID. **CVE ID : CVE-2019-10445**	9-10-16/#SECURITY-1607	
cadence_vmanager					
Improper Certificate Validation	16-10-2019	6.4	Jenkins Cadence vManager Plugin 2.7.0 and earlier disabled SSL/TLS and hostname verification globally for the Jenkins master JVM. **CVE ID : CVE-2019-10446**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1615	A-JEN-CADE-041119/303
oracle_cloud_infrastructure_compute_classic					
Cross-Site Request Forgery (CSRF)	16-10-2019	4.3	A cross-site request forgery vulnerability in Jenkins Oracle Cloud Infrastructure Compute Classic Plugin allows attackers to connect to an attacker-specified URL using attacker-specified credentials. **CVE ID : CVE-2019-10456**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1462	A-JEN-ORAC-041119/304
Incorrect Permission Assignment for Critical Resource	16-10-2019	4	A missing permission check in Jenkins Oracle Cloud Infrastructure Compute Classic Plugin allows attackers with Overall/Read permission to connect to an attacker-specified URL using	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1462	A-JEN-ORAC-041119/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker-specified credentials. **CVE ID : CVE-2019-10457**		
deploy_weblogic					
Cross-Site Request Forgery (CSRF)	23-10-2019	6.8	A cross-site request forgery vulnerability in Jenkins Deploy WebLogic Plugin allows attackers to connect to an attacker-specified URL using attacker-specified credentials, or determine whether a file or directory with an attacker-specified path exists on the Jenkins master file system. **CVE ID : CVE-2019-10464**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-820	A-JEN-DEPL-041119/306
Incorrect Default Permissions	23-10-2019	4	A missing permission check in Jenkins Deploy WebLogic Plugin allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials, or determine whether a file or directory with an attacker-specified path exists on the Jenkins master file system. **CVE ID : CVE-2019-10465**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-820	A-JEN-DEPL-041119/307
soasta_cloudtest					
Cleartext Storage of Sensitive	16-10-2019	4	Jenkins SOASTA CloudTest Plugin stores credentials unencrypted in its global configuration file on the	https://jenkins.io/security/advisory/2019-10-	A-JEN-SOAS-041119/308

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-2019-10451**	16/#SECURITY-1439	
sofy.ai					
Cleartext Storage of Sensitive Information	16-10-2019	4	Jenkins Sofy.AI 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-2019-10447**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1431	A-JEN-SOFY-041119/309
extensive_testing					
Insufficiently 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://jenkins.io/security/advisory/2019-10-16/#SECURITY-1432	A-JEN-EXTE-041119/310
fortify_on_demand					
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://jenkins.io/security/advisory/2019-10-16/#SECURITY-1433	A-JEN-FORT-041119/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission, or access to the master file system. **CVE ID : CVE-2019-10449**		
elasticbox_ci					
Cleartext Storage of Sensitive Information	16-10-2019	2.1	Jenkins ElasticBox CI 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**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1434	A-JEN-ELAS-041119/312
view26_test-reporting					
Cleartext Storage of Sensitive Information	16-10-2019	4	Jenkins View26 Test-Reporting 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-2019-10452**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1440	A-JEN-VIEW-041119/313
puppet_enterprise_pipeline					
Improper Input Validation	16-10-2019	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://jenkins.io/security/advisory/2019-10-16/#SECURITY-918	A-JEN-PUPP-041119/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10458		
bitbucket_oauth					
Insufficientl y Protected Credentials	23-10-2019	2.1	Jenkins Bitbucket OAuth 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**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1546	A-JEN-BITB-041119/315
libvirt_slaves					
Cross-Site Request Forgery (CSRF)	23-10-2019	6.8	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-2019-10471**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1014%20(1)	A-JEN-LIBV-041119/316
Incorrect Default Permissions	23-10-2019	4	A missing permission check in Jenkins Libvirt Slaves Plugin allows attackers with Overall/Read permission to connect to an attacker-specified SSH server using attacker-specified credentials IDs obtained through another method, capturing credentials	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1014%20(1)	A-JEN-LIBV-041119/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stored in Jenkins. **CVE ID : CVE-2019-10472**		
Incorrect Default Permissions	23-10-2019	4	A missing permission check in Jenkins Libvirt Slaves Plugin in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2019-10473**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1014%20(2)	A-JEN-LIBV-041119/318
global_post_script					
Incorrect Default Permissions	23-10-2019	4	A missing permission check in Jenkins Global Post Script Plugin in allowed users with Overall/Read access to list the scripts available to the plugin stored on the Jenkins master file system. **CVE ID : CVE-2019-10474**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1073	A-JEN-GLOB-041119/319
google_oauth_credentials					
Information Exposure	16-10-2019	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://jenkins.io/security/advisory/2019-10-16/#SECURITY-1583	A-JEN-GOOG-041119/320
crx_content_package_deployer					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	16-10-2019	6.8	A cross-site request forgery vulnerability in Jenkins CRX Content Package Deployer Plugin 1.8.1 and earlier allowed attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10437**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1006%20(1)	A-JEN-CRX_-041119/321
Incorrect Permission Assignment for Critical Resource	16-10-2019	4	A missing permission check in Jenkins CRX Content Package Deployer Plugin 1.8.1 and earlier allowed 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. **CVE ID : CVE-2019-10438**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1006%20(1)	A-JEN-CRX_-041119/322
Insufficiently Protected Credentials	16-10-2019	4	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://jenkins.io/security/advisory/2019-10-16/#SECURITY-1006%20(2)	A-JEN-CRX_-041119/323

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
			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. **CVE ID : CVE-2019-10440**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1427	A-JEN-NEOL-041119/324
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-2019-10441**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1484	A-JEN-ICES-041119/325
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-2019-10442**	https://jenkins.io/security/advisory/2019-10-16/#SECURITY-1484	A-JEN-ICES-041119/326

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://jenkins.io/security/advisory/2019-10-16/#SECURITY-1436	A-JEN-ICES-041119/327
delphix					
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://jenkins.io/security/advisory/2019-10-16/#SECURITY-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://jenkins.io/security/advisory/2019-10-16/#SECURITY-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://jenkins.io/security/advisory/2019-10-16/#SECURIT	A-JEN-RUND-041119/330

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using attacker-specified credentials. **CVE ID : CVE-2019-10455**	Y-1460	
mattermost_notification					
Insufficiently Protected Credentials	23-10-2019	4	Jenkins Mattermost Notification Plugin 2.7.0 and earlier stored webhook URLs containing a secret token unencrypted in its global configuration file and 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-2019-10459**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1628	A-JEN-MATT-041119/331
dynatrace_application_monitoring					
Insufficiently 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 Jenkins master where they could be viewed by users with access to the master file system. **CVE ID : CVE-2019-10461**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1477	A-JEN-DYNA-041119/332
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://jenkins.io/security/advisory/2019-10-23/#SECURITY-	A-JEN-DYNA-041119/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect to an attacker-specified URL using attacker-specified credentials. **CVE ID : CVE-2019-10462**	1483%20(1)	
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://jenkins.io/security/advisory/2019-10-23/#SECURITY-1483%20(2)	A-JEN-DYNA-041119/334
360_fireline					
Improper Restriction of XML External Entity Reference ('XXE')	23-10-2019	5.5	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-2019-10466**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-822	A-JEN-360_-041119/335
sonar_gerrit					
Insufficiently 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://jenkins.io/security/advisory/2019-10-23/#SECURIT	A-JEN-SONA-041119/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10467**	Y-1003	
kubernetes_ci					
Cross-Site Request Forgery (CSRF)	23-10-2019	6.8	A cross-site request forgery vulnerability in Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10468**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1005%20(1)	A-JEN-KUBE-041119/337
Incorrect Default Permissions	23-10-2019	4	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. **CVE ID : CVE-2019-10469**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1005%20(1)	A-JEN-KUBE-041119/338
Incorrect Default Permissions	23-10-2019	4	A missing permission check in Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin	https://jenkins.io/security/advisory/2019-10-	A-JEN-KUBE-041119/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2019-10470**	23/#SECURITY-1005%20(2)	
build-metrics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	A reflected cross-site scripting vulnerability in Jenkins build-metrics Plugin allows attackers to inject arbitrary HTML and JavaScript into web pages provided by this plugin. **CVE ID : CVE-2019-10475**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1490	A-JEN-BUIL-041119/340
zulip					
Insufficiently 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 system. **CVE ID : CVE-2019-10476**	https://jenkins.io/security/advisory/2019-10-23/#SECURITY-1621	A-JEN-ZULI-041119/341
K7computing					
k7_antivirus_premium					
Improper Privilege Management	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-K7_A-041119/342

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 inter-process communication with a service process. **CVE ID : CVE-2019-16897**		
k7_total_security					
Improper Privilege Management	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 Management	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Kubernetes					
kubernetes					
Improper Input Validation	17-10-2019	5	Improper input validation in the Kubernetes API server in versions v1.0-1.12 and versions prior to v1.13.12, v1.14.8, v1.15.5, and v1.16.2 allows authorized users to send malicious YAML or JSON payloads, causing the API server to consume excessive CPU or memory, potentially crashing and becoming unavailable. Prior to v1.14.0, default RBAC policy authorized anonymous users to submit requests that could trigger this vulnerability. Clusters upgraded from a version prior to v1.14.0 keep the more permissive policy by default for backwards compatibility. **CVE ID : CVE-2019-**	https://github.com/kubernetes/kubernetes/issues/83253	A-KUB-KUBE-041119/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11253		
Libarchive					
libarchive					
Use After Free	24-10-2019	5	archive_read_format_rar_read_data in archive_read_support_format_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**	N/A	A-LIB-LIBA-041119/346
libpl_droidsonroids_gif_project					
libpl_droidsonroids_gif					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-10-2019	7.5	A heap buffer overflow 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-2019-11933**	https://www.facebook.com/security/advisories/cve-2019-11933	A-LIB-LIBP-041119/347
libpod_project					
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/A	A-LIB-LIBP-041119/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could create a 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**		
Libssh2					
libssh2					
Integer Overflow or Wraparound	21-10-2019	5.8	In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. **CVE ID : CVE-2019-17498**	N/A	A-LIB-LIBS-041119/349
Limesurvey					
limesurvey					
Improper Neutralization of Input During Web Page Generation	16-10-2019	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-LIME-041119/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attackers to inject arbitrary web script or HTML via the tolang parameter, as demonstrated by the index.php/admin/translate/sa/index/surveyid/336819/lang/ PATH_INFO. **CVE ID : CVE-2019-17660**		
loofah_project					
loofah					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-10-2019	3.5	In the Loofah gem for Ruby through v2.3.0 unsanitized JavaScript may occur in sanitized output when a crafted SVG element is republished. **CVE ID : CVE-2019-15587**	https://github.com/flavorjones/loofah/issues/171	A-LOO-LOOF-041119/351
managewp					
broken_link_checker					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	The broken-link-checker plugin through 1.11.8 for WordPress (aka Broken Link Checker) is susceptible to Reflected XSS due to improper encoding and insertion of an HTTP GET parameter into HTML. The filter function on the page listing all detected broken links can be exploited by providing an XSS payload in the s_filter GET parameter in a filter_id=search request. NOTE: this is an end-of-life	N/A	A-MAN-BROK-041119/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product. **CVE ID : CVE-2019-16521**		
Improper Neutralization 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=view-broken-links s_filter parameter in a search action. **CVE ID : CVE-2019-17207**	N/A	A-MAN-BROK-041119/353
mapr					
mapr					
Improper Input Validation	24-10-2019	7.5	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 can force the MapR CLDB	N/A	A-MAP-MAPR-041119/354

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-2019-17676**	N/A	A-MET-METI-041119/355
Microfocus					
netiq_self_service_password_reset					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	22-10-2019	4.3	Man-in-the-middle 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**	N/A	A-MIC-NETI-041119/356
mindpalette					
natemail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	4.3	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-2019-13392**	N/A	A-MIN-NATE-041119/357
mp3gain_project					
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-MP3G-041119/358

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_runtime					
Deserialization 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 **CVE ID : CVE-2019-13116**	N/A	A-MUL-MULE-041119/359
Nchsoftware					
express_accounts_accounting					
Improper Neutralization 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. **CVE ID : CVE-2019-16330**	N/A	A-NCH-EXPR-041119/360
Netapp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
snapmanager					
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2983**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in 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 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-2019-2987**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
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; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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 (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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 ID : CVE-2019-2999**		
N/A	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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2958**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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,	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 some of Java SE, Java SE	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-SNAP-041119/377

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://security.netapp.com/advisory/ntap-20191017-0002/	A-NET-SNAP-041119/378

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). **CVE ID : CVE-2019-2922**		
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://security.netapp.com/advisory/ntap-20191017-0002/	A-NET-SNAP-041119/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
oncommand_workflow_automation					
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://security.netapp.com/advisory/ntap-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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows 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: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).		

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
			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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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.	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/385

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 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 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),	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/387

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
			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-2019-2987**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
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; 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2999**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE	https://security.netapp.com/advisory/nta	A-NET-ONCO-041119/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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:N/UI:N/S:U/C:N/I:H/A:N).	p-20191017-0001/	

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
			CVE ID : CVE-2019-2958		
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 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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/394

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-2019-2962**		
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:	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2964**		
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.	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ONCO-041119/397

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_software_management_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://security.netapp.com/advisory/ntap-20191017-0003/, https://support.f5.com/csp/article/K53746212?utm_source=f5support&utm_medium=RSS, https://www.sudo.ws/alerts/minus_1_uid.html	A-NET-ELEM-041119/398
e-series_santricity_os_controller					
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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/UI:R/S:U/C:N/I:N/A:L).		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2945		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-2987**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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-2019-2992**		
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; 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.	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/410

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	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2999**		
N/A	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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2958**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/414

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 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**		
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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/415

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_santricity_storage_manager					
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (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 SE product of Oracle Java	https://security.netapp.com	A-NET-E-SE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L).	/advisory/ntap-20191017-0001/	041119/418

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
			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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/419

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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/421

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 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 access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2987**		
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),	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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.	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
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; 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/426

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 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 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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2999**		
N/A	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:	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2958**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded	https://security.netapp.com	A-NET-E-SE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:	/advisory/ntap-20191017-0001/	041119/429

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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/430

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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 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.	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/432

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_santricity_unified_manager					
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (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 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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-	A-NET-E-SE-041119/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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**	0001/	

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
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/438

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-2019-2983**		
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 access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in 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 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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 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**	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/441

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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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; 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2999**		
N/A	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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2958**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2962**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2973**		
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	https://security.netapp.com/advisory/ntap-20191017-	A-NET-E-SE-041119/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 impacts). CVSS Vector:	0001/	

Weakness	Publish Date	CVSS	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_santricity_web_services_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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/452

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 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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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-2019-2981**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2983**		
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:	https://security.netapp.com/advisory/ntap-20191017-	A-NET-E-SE-041119/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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 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-2019-2987**	0001/	
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:	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
N/A	16-10-2019	4.3	Vulnerability in the Oracle GraalVM Enterprise	https://security.netapp.com	A-NET-E-SE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	/advisory/ntap-20191017-0001/	041119/458
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
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;	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/460

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		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 ID : CVE-2019-2999**		
N/A	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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2958**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2962**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2973**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-E-SE-041119/466

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_unified_manager					
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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ACTI-041119/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/nta	A-NET-ACTI-041119/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	p-20191017-0001/	

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://security.netapp.com/advisory/ntap-20191017-0001/	A-NET-ACTI-041119/469

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-2019-2973**		
NSA					
ghidra					
Untrusted Search Path	16-10-2019	4.4	NSA Ghidra through 9.0.4 uses a potentially untrusted search path. When executing Ghidra from a given path, the Java process working directory is set to this path. Then, when launching the Python interpreter via the "Ghidra Codebrowser > Window > Python" option, Ghidra will try to execute the cmd.exe program from this working directory. **CVE ID : CVE-2019-17664**	N/A	A-NSA-GHID-041119/470
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-GHID-041119/471
Openafs					
openafs					
Deserialization 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	N/A	A-OPE-OPEN-041119/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			series of VOTE_Debug RPC calls to crash a database server within the SVOTE_Debug RPC handler. **CVE ID : CVE-2019-18601**		
Information Exposure	29-10-2019	5	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to an information disclosure vulnerability because uninitialized scalars are sent over the network to a peer. **CVE ID : CVE-2019-18602**	N/A	A-OPE-OPEN-041119/473
Information Exposure	29-10-2019	4.3	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. **CVE ID : CVE-2019-18603**	N/A	A-OPE-OPEN-041119/474
Open-emr					
openemr					
Improper Neutralization 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-OPEN-041119/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			providerID parameter. **CVE ID : CVE-2019-16404**		
Improper Neutralization 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 Neutralization 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)	18-10-2019	6.8	OpenWRT firmware version 18.06.4 is vulnerable to CSRF via wireless/radio0.network1, wireless/radio1.network1, firewall, firewall/zones, firewall/forwards, firewall/rules, network/wan, network/wan6, or network/lan under /cgi-bin/luci/admin/network/. **CVE ID : CVE-2019-17367**	https://github.com/openwrt/luci/commit/f8c6eb67cd9da09ee20248fec6ab742069635e47	A-OPE-OPEN-041119/478
Oracle					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
retail_customer_management_and_segmentation_foundation					
Incorrect Authorization	16-10-2019	4.9	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Segment). The supported version that is affected is 17.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. 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 Customer Management and Segmentation Foundation accessible data as well as unauthorized read access to a subset of Oracle Retail Customer Management and Segmentation Foundation accessible data. CVSS 3.0 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).	N/A	A-ORA-RETA-041119/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2883		
Information Exposure	16-10-2019	4.3	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Segment). The supported version that is affected is 17.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Customer Management and Segmentation Foundation 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-2019-2884**	N/A	A-ORA-RETA-041119/480
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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/481

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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2911**		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.27 and prior and 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-2019-2914**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/483
Incorrect Authorization	16-10-2019	5	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-MYSQ-041119/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to 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). **CVE ID : CVE-2019-2920**		
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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-2019-2923**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/486
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	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 5.7.27 and prior and 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 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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2938**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/488
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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2946**		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 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).	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 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://security.netapp.com/advisory/ntap-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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2991**		
N/A	16-10-2019	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit 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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/493

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). **CVE ID : CVE-2019-2997**	https://security.netapp.com/advisory/ntap-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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2998**		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.16 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-2019-3003**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/496
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-3004**		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection). 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 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 4.4 (Availability impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/498

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://security.netapp.com/advisory/ntap-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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-3018**		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.16 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-2019-2950**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/501
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component:	https://security.netapp.com/advisory/nta	A-ORA-MYSQ-041119/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server: Security: Encryption). 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-2019-2957**	p-20191017-0002/	
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 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 ability to cause a hang or frequently repeatable crash (complete DOS) of	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2960**		
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). **CVE ID : CVE-2019-2963**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/504
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	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/505

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). **CVE ID : CVE-2019-2966**		
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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/506

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). **CVE ID : CVE-2019-2968**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/507
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://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 6.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2969**		
N/A	16-10-2019	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). 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 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-2019-2974**	https://security.netapp.com/advisory/ntap-20191017-0002/	A-ORA-MYSQ-041119/509
jdk					
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded	https://security.netapp.com	A-ORA-JDK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	/advisory/ntap-20191017-0001/	041119/510

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
			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://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supplies data to the APIs. 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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/513

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 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2983**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: 2D).	https://security.netapp.com/advisory/nta	A-ORA-JDK-041119/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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 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-2019-2987**	p-20191017-0001/	
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D).	https://security.netapp.com/advisory/ntap-20191017-	A-ORA-JDK-041119/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). 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**	0001/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 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**	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/520
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
N/A	16-10-2019	4	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Deployment). The	https://security.netapp.com/advisory/ntap-20191017-	A-ORA-JDK-041119/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported version that is 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	0001/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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**		
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),	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 ID : CVE-2019-2999**		
N/A	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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/524

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 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2958**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2962**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	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-2019-2973**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JDK-041119/528

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). **CVE ID : CVE-2019-2975**		
jre					
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security).	https://security.netapp.com/advisory/ntap-20191017-	A-ORA-JRE-041119/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2894**	0001/	

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
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://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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,	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2983**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: 2D). Supported versions that	https://security.netapp.com/advisory/ntap-20191017-	A-ORA-JRE-041119/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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 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-2019-2987**	0001/	
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://security.netapp.com/advisory/ntap-20191017-	A-ORA-JRE-041119/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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**	0001/	

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
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 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**	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/539
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
N/A	16-10-2019	4	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Deployment). The	https://security.netapp.com/advisory/ntap-20191017-	A-ORA-JRE-041119/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported version that is 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	0001/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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**		
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),	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 ID : CVE-2019-2999**		
N/A	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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/543

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 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2958**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2962**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	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-2019-2973**		
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://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-JRE-041119/547

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). **CVE ID : CVE-2019-2975**		
outside_in_technology					
N/A	16-10-2019	7.5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component:	N/A	A-ORA-OUTS-041119/548

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,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2901**		
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	N/A	A-ORA-OUTS-041119/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2902**		
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	N/A	A-ORA-OUTS-041119/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2903**		
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	N/A	A-ORA-OUTS-041119/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2970**		
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	N/A	A-ORA-OUTS-041119/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2971**		

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
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-ORA-OUTS-041119/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2972**		
content_manager					
N/A	16-10-2019	5	Vulnerability in the Oracle Content Manager product of Oracle E-Business Suite (component: Content). 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 Content Manager. While the vulnerability is in Oracle Content Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Content Manager accessible data. CVSS 3.0 Base Score 5.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N). **CVE ID : CVE-2019-3022**	N/A	A-ORA-CONT-041119/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vm_virtualbox					
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). **CVE ID : CVE-2019-2926**	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). **CVE ID : CVE-2019-2944**		
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	N/A	A-ORA-VM_V-041119/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2019-2984**		
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. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	N/A	A-ORA-VM_V-041119/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2019-3002**		
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. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox. CVSS 3.0 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:	N/A	A-ORA-VM_V-041119/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2019-3005**		
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 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 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-3017**	N/A	A-ORA-VM_V-041119/560
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 low	N/A	A-ORA-VM_V-041119/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2019-3021**		
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 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	N/A	A-ORA-VM_V-041119/562

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	Description & CVE ID	Patch	NCIIPC ID
			L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-3028**		
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. While the vulnerability is in Oracle VM VirtualBox, 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 VM VirtualBox accessible data. CVSS 3.0 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2019-3031**	N/A	A-ORA-VM_V-041119/564
primavera_p6_enterprise_project_portfolio_management					
N/A	16-10-2019	3.5	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component:	N/A	A-ORA-PRIM-041119/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Web Access). Supported versions that are affected are 17.1.0-17.12.12. Easily exploitable vulnerability allows low privileged 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 access to critical data or complete access to all Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2019-2976**		
N/A	16-10-2019	5.8	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported	N/A	A-ORA-PRIM-041119/566

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	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N/UI:R/S:C/C:H/I:H/A:N). **CVE ID : CVE-2019-3020**		
database_server					
Improper Input Validation	16-10-2019	4.3	Vulnerability in the Java VM 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. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java VM. While the vulnerability is in Java VM, 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 Java VM 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-2019-2909**	N/A	A-ORA-DATA-041119/567
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-DATA-041119/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 ID : CVE-2019-2913**		
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 accessible data. CVSS 3.0	N/A	A-ORA-DATA-041119/569

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Session, Execute on DBMS_ADVISOR privilege with network access via OracleNet 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 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2019-2734**		
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 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 unauthorized ability to	N/A	A-ORA-DATA-041119/572

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	Description & CVE ID	Patch	NCIIPC ID
			L/UI:R/S:U/C:N/I:L/A:L). **CVE ID : CVE-2019-2955**		
N/A	16-10-2019	3.5	Vulnerability in the Core RDBMS (jackson-databind) component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via multiple protocols to compromise Core RDBMS (jackson-databind). 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 hang or frequently repeatable crash (complete DOS) of Core RDBMS (jackson-databind). CVSS 3.0 Base Score 5.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2956**	N/A	A-ORA-DATA-041119/574
flexcube_direct_banking					
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-FLEX-041119/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Payments). 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 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). **CVE ID : CVE-2019-2979**		
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-FLEX-041119/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2980**		
siebel_crm					
N/A	16-10-2019	5	Vulnerability in the Siebel Core - DB Deployment and Configuration product of Oracle Siebel CRM (component: Install - Configuration). Supported versions that are affected are 19.8 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Core - DB Deployment and Configuration. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel Core - DB Deployment and Configuration 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).	N/A	A-ORA-SIEB-041119/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2965		
business_intelligence_publisher					
N/A	16-10-2019	5.8	Vulnerability in the BI Publisher (formerly XML Publisher) product of Oracle Fusion Middleware (component: Mobile Service). 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 HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS	N/A	A-ORA-BUSI-041119/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
marketing					
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

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	Patch	NCIIPC ID
			CVE ID : CVE-2019-3000		
business_intelligence					
N/A	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-BUSI-041119/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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-BUSI-041119/583
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	N/A	A-ORA-BUSI-041119/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated 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 access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2019-2905**		
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-BUSI-041119/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise 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**		
application_object_library					
N/A	16-10-2019	5	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). CVSS Vector:	N/A	A-ORA-APPL-041119/586

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					
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

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_outbound_telephony					
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

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_cruise_dining_room_management					
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	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2019-2953**		
data_integrator					
N/A	16-10-2019	4	Vulnerability in the Oracle Data Integrator product of Oracle Fusion Middleware (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 HTTP to compromise Oracle Data Integrator. Successful attacks of this vulnerability can result in 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/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2943**	N/A	A-ORA-DATA-041119/590
food_and_beverage_applications					
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 Inventory	N/A	A-ORA-FOOD-041119/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Integration privilege with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2019-2947**		
Incorrect Authorization	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-FOOD-041119/592

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). **CVE ID : CVE-2019-2952**		
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
graalvm					
N/A	16-10-2019	4	Vulnerability in the Oracle 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-ORA-GRAA-041119/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2019-2986**		
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 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**	https://security.netapp.com/advisory/ntap-20191017-0001/	A-ORA-GRAA-041119/595
field_service					
Improper Authenticati	16-10-2019	4.3	Vulnerability in the Oracle Field Service product of	N/A	A-ORA-FIEL-

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_framework					
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-2935**		
retail_xstore_point_of_service					
N/A	16-10-2019	2.6	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 accessible data as well as	N/A	A-ORA-RETA-041119/598

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	Description & CVE ID	Patch	NCIIPC ID
			Forms 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-2019-2886**		
enterprise_manager					
N/A	16-10-2019	6	Vulnerability in the Enterprise Manager for Exadata product of Oracle Enterprise Manager (component: Exadata Plug-In Deploy and Ins). Supported versions that are affected are 12.1.0.5.0, 13.2.2.0.0, 13.3.1.0.0 and 13.3.2.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager for Exadata. Successful attacks of this vulnerability can result in takeover of Enterprise Manager for Exadata. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2895**	N/A	A-ORA-ENTE-041119/600
micros_relate_customer_relationship_management_software					
N/A	16-10-2019	4.3	Vulnerability in the MICROS Relate CRM	N/A	A-ORA-MICR-041119/601

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**		
application_development_framework					
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

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	Description & CVE ID	Patch	NCIIPC ID
			N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2904**		
jdeveloper					
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 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	A-ORA-JDEV-041119/604
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-JDEV-041119/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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					
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-ORA-WEB_-041119/606

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					
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_data_relationship_management					
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
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

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_enterprise_human_capital_management_human_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/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2951**	N/A	A-ORA-PEOP-041119/610
hyperion_financial_reporting					
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 exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion	N/A	A-ORA-HYPE-041119/611

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). **CVE ID : CVE-2019-2959**		
peoplesoft_enterprise_scm_eprocurement					
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

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_digital_experience					
Incorrect Authorization	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_base					
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 Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2019-3024**		
hospitality_res_3700					
N/A	16-10-2019	6.8	Vulnerability in the Oracle Hospitality RES 3700 component of Oracle Food and Beverage Applications. The supported version that is affected is 5.7. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality RES 3700. While the vulnerability is in Oracle Hospitality RES 3700, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality RES 3700. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-3025**	N/A	A-ORA-HOSP-041119/615
weblogic_server					
Information Exposure	16-10-2019	4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported	N/A	A-ORA-WEBL-041119/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2019-2887**		
Information Exposure	16-10-2019	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: EJB Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0	N/A	A-ORA-WEBL-041119/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2888**		
N/A	16-10-2019	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). 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 WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-WEBL-041119/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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). **CVE ID : CVE-2019-2890**	N/A	A-ORA-WEBL-041119/619
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-WEBL-041119/620

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_reporting_and_analytics					
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and 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-2019-2934**		
N/A	16-10-2019	4.9	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. Difficult to exploit 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 6.8 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-HOSP-041119/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2019-2936**		
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 Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and 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**	N/A	A-ORA-HOSP-041119/623
peoplesoft_enterprise_peopletools					

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	Description & CVE ID	Patch	NCIIPC ID
N/A	16-10-2019	4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Tree Manager). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2019-2932**	N/A	A-ORA-PEOP-041119/627
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	N/A	A-ORA-PEOP-041119/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2985**		
N/A	16-10-2019	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Performance Monitor). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated	N/A	A-ORA-PEOP-041119/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-3014**		
N/A	16-10-2019	4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows low privileged	N/A	A-ORA-PEOP-041119/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools 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-2019-3015**		
N/A	16-10-2019	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Stylesheet). 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,	N/A	A-ORA-PEOP-041119/631

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). **CVE ID : CVE-2019-3023**		
Paloaltonetworks					
globalprotect					
Improper Privilege Management	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://securityadvisories.paloaltonetworks.com/Home/Detail/197	A-PAL-GLOB-041119/632
Improper Privilege Management	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://securityadvisories.paloaltonetworks.com/Home/Detail/200	A-PAL-GLOB-041119/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Philips					
intellispace_perinatal					
Exposure of Resource to Wrong Sphere	25-10-2019	7.2	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-2019-13546**	N/A	A-PHI-INTE-041119/634
PHP					
php					
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	https://bugs.php.net/bug.php?id=78599, https://support.f5.com/csp/article/K75408500?utm_source=f5supp	A-PHP-PHP-041119/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution. **CVE ID : CVE-2019-11043**	ort&utm_medium=RSS	
Pivotal					
reactor_netty					
Insufficientl y Protected Credentials	17-10-2019	5	Pivotal Reactor Netty, versions prior to 0.8.11, passes headers through redirects, including authorization ones. A remote unauthenticated malicious user may gain access to credentials for a different server than they have access to. **CVE ID : CVE-2019-11284**	https://pivotal.io/security/cve-2019-11284	A-PIV-REAC-041119/636
pivotal_software					
cloud_foundry_uaa					
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://www.cloudfoundry.org/blog/cve-2019-11282	A-PIV-CLOU-041119/637
rabbitmq					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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://pivotal.io/security/cve-2019-11281	A-PIV-RABB-041119/638
cloud_foundry_cf-deployment					
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://www.cloudfoundry.org/blog/cve-2019-11282	A-PIV-CLOU-041119/639
Information Exposure	23-10-2019	4	Cloud Foundry SMB Volume, versions prior to	https://www.cloudfoundry.	A-PIV-CLOU-

Weakness	Publish 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/cve-2019-11283	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	3.5	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://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10209, https://www.postgresql.org/about/news/	A-POS-POST-041119/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1960/	
Proftpd					
proftpd					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-10-2019	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**	N/A	A-PRO-PROF-041119/643
Python					
python					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-10-2019	4.3	An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
QT					
qtbase					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-10-2019	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. **CVE ID : CVE-2019-18281**	N/A	A-QT-QTBA-041119/645
rambox					
rambox					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-10-2019	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	18-10-2019	5	An issue was discovered in	https://githu	A-RAT-RATP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Ratpack before 1.7.5. Due to a misuse of the Netty library class DefaultHttpHeaders, there is no validation that headers lack HTTP control characters. Thus, if untrusted data is used to construct HTTP headers with Ratpack, HTTP Response Splitting can occur. **CVE ID : CVE-2019-17513**	b.com/ratpack/ratpack/releases/tag/v1.7.5, https://github.com/ratpack/ratpack/security/advisories/GHSA-mvqp-q37c-wf9j	041119/647
rconfig					
rconfig					
Improper Neutralization 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-RCON-041119/648
Improper Neutralization 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-RCON-041119/649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command execution. **CVE ID : CVE-2019-16663**		
repetier-server					
repetier-server					
Unrestricted Upload of File with Dangerous Type	25-10-2019	10	RepetierServer.exe in 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**	https://www.repetier-server.com/knowledgebase/security-advisory/	A-REP-REPE-041119/650
reportlab					
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 color="' followed by arbitrary Python code. **CVE ID : CVE-2019-**	N/A	A-REP-REPO-041119/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17626		
restaurant_management_system_project					
restaurant_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	4.3	Sourcecodester Restaurant Management System 1.0 allows XSS via the "send a message" screen. **CVE ID : CVE-2019-18415**	N/A	A-RES-REST-041119/652
Improper Neutralization 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-REST-041119/653
rocket.chat					
rocket.chat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-10-2019	4.3	Rocket.Chat before 2.1.0 allows XSS via a URL on a ![title] line. **CVE ID : CVE-2019-17220**	N/A	A-ROC-ROCK-041119/654
sagemath					
sagemathcell					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			application. Malicious actors can execute arbitrary commands on the underlying operating system, as demonstrated by an __import__('os').popen('whoami').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					
Unrestricted Upload of File with Dangerous Type	24-10-2019	6.5	** DISPUTED ** admin/app/mediamanager in Schlix CMS 2.1.8-7 allows Authenticated Unrestricted File Upload, leading to remote code execution. NOTE: "While inadvertently allowing a PHP file to be uploaded via Media Manager was an oversight, it still requires 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**	N/A	A-SCH-CMS-041119/656
semperplugins					
all_in_one_seo_pack					
Improper Neutralizati	16-10-2019	3.5	The all-in-one-seo-pack plugin before 3.2.7 for	N/A	A-SEM-ALL_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			WordPress (aka All in One SEO Pack) is susceptible to Stored XSS due to improper encoding of the SEO-specific description for posts provided by the plugin via unsafe placeholder replacement. **CVE ID : CVE-2019-16520**		041119/657
sequelizejs					
sequelize					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-10-2019	7.5	Sequelize all versions prior to 3.35.1, 4.44.3, and 5.8.11 are vulnerable to SQL Injection due to JSON path keys not being properly escaped for the MySQL/MariaDB dialects. **CVE ID : CVE-2019-10748**	N/A	A-SEQ-SEQU-041119/658
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-10-2019	7.5	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-SEQU-041119/659
Improper Neutralization 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://snyk.io/vuln/SNYK-JS-SEQUELIZE-459751,	A-SEQ-SEQU-041119/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			MariaDB and SQLite. **CVE ID : CVE-2019-10752**		
sitemagic					
sitemagic					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	Sitemagic CMS 4.4.1 is affected by a Cross-Site-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)	23-10-2019	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_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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://typo3.org/security/advisory/typo3-ext-sa-2019-017/	A-SLU-SLUB-041119/663
Sonatype					
nexus_iq_server					
Unrestricted Upload of File with Dangerous Type	21-10-2019	9	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**	https://support.sonatype.com/hc/en-us/articles/360036132453	A-SON-NEXU-041119/664
nexus_repository_manager					
Improper Privilege Management	16-10-2019	6.5	Sonatype Nexus Repository Manager 2.x before 2.14.15 allows Remote Code Execution. **CVE ID : CVE-2019-15893**	https://support.sonatype.com/hc/en-us/articles/360035055794	A-SON-NEXU-041119/665
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	https://support.sonatype.com/hc/en-us/articles/3	A-SON-NEXU-041119/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			before 72, has remote code execution. **CVE ID : CVE-2019-16530**	60036132453	
sourcecodester					
restaurant_management_system					
Cross-Site Request Forgery (CSRF)	24-10-2019	6.8	Sourcecodester Restaurant Management System 1.0 is affected by an admin/staff-exec.php 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 or adding a staff entry via a crafted HTML page. **CVE ID : CVE-2019-18414**	N/A	A-SOU-REST-041119/667
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-REST-041119/668
online_grading_system					
Cross-Site	23-10-2019	6.8	Sourcecodester Online	N/A	A-SOU-ONLI-

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/controller.php?action=add URI. **CVE ID : CVE-2019-18280**		041119/669
Improper Neutralization 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_project					
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/typo3-ext-sa-2019-018/	A-SR_-SR_F-041119/671

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://security.netapp.com/advisory/ntap-20191017-0003/, https://support.f5.com/csp/article/K53746212?utm_source=f5support&utm_medium=RSS, https://www.sudo.ws/alerts/minus_1_uid.html	A-SUD-SUDO-041119/672
Symantec					
messaging_gateway					
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://support.symantec.com/en_US/article.SYMSA1482.html	A-SYM-MESS-041119/673
Teamviewer					
teamviewer					
Untrusted	24-10-2019	6.9	A DLL side loading	https://comm	A-TEA-TEAM-

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.teamviewer.com/t5/Announcements/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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-3982		
theia_xml_extension_project					
theia_xml_extension					
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-2019-18212**	https://github.com/angelozerr/lsp4xml/blob/master/CHANGELOG.md#others	A-THE-THEI-041119/676
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/LSPXMLParserConfiguration.java. **CVE ID : CVE-2019-18213**	https://github.com/angelozerr/lsp4xml/blob/master/CHANGELOG.md#others	A-THE-THEI-041119/677
themooltipass					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
moolticute					
Cleartext Transmission of Sensitive Information	22-10-2019	4.3	Stephan Mooltipass Moolticute through 0.42.1 (and possibly earlier versions) has Incorrect Access Control. **CVE ID : CVE-2019-12967**	N/A	A-THE-MOOL-041119/678
Thycotic					
secret_server					
Server-Side Request Forgery (SSRF)	23-10-2019	7.5	An SSRF issue was discovered in the legacy Web launcher in Thycotic Secret Server before 10.7. **CVE ID : CVE-2019-18355**	N/A	A-THY-SECR-041119/679
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	An XSS issue was discovered in Thycotic Secret Server before 10.7 (issue 1 of 2). **CVE ID : CVE-2019-18356**	N/A	A-THY-SECR-041119/680
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-10-2019	4.3	An XSS issue was discovered in Thycotic Secret Server before 10.7 (issue 2 of 2). **CVE ID : CVE-2019-18357**	N/A	A-THY-SECR-041119/681
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which can potentially result code execution.. This attack appear to be exploitable via network connectivity. **CVE ID : CVE-2019-15678**		
Out-of-bounds Write	29-10-2019	7.5	TightVNC code version 1.3.10 contains heap buffer overflow in InitialiseRFBConnection function, which can potentially result code execution. This attack appear to be exploitable via network connectivity. **CVE ID : CVE-2019-15679**	N/A	A-TIG-TIGH-041119/683
NULL Pointer Dereference	29-10-2019	5	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-2019-15680**	N/A	A-TIG-TIGH-041119/684
tomedo					
server					
Insufficiently Protected Credentials	18-10-2019	5	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-SERV-041119/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it possible to base64 decode the sniffed credentials and discover the username and password. **CVE ID : CVE-2019-17393**		
topmeeting					
topmeeting					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-10-2019	5	A SQL injection vulnerability was discovered in TOPMeeting before version 8.8 (2019/08/19). An attacker can use a union based injection query string though a search meeting room feature to get databases schema and username/password. **CVE ID : CVE-2019-13409**	https://tvn.twcert.org.tw/taiwanvn/TVN-201907001, https://www.twcert.org.tw/en/cp-128-3019-f0dd8-2.html	A-TOP-TOPM-041119/686
Information Exposure	17-10-2019	5	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://tvn.twcert.org.tw/taiwanvn/TVN-201907002, https://www.twcert.org.tw/en/cp-128-3020-27eb5-2.html	A-TOP-TOPM-041119/687
totemo					
totemodata					
Improper Neutralization 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-TOTE-041119/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			**17189**		
Trendmicro					
deep_security					
Information Exposure	17-10-2019	4.3	The Deep Security Manager application (Versions 10.0, 11.0 and 12.0), when configured in a certain way, may transmit initial LDAP communication in clear text. This may result in confidentiality impact but does not impact integrity or availability. **CVE ID : CVE-2019-15626**	N/A	A-TRE-DEEP-041119/689
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-DEEP-041119/690
anti-threat_toolkit					
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-ANTI-041119/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same directory, potentially leading to arbitrary remote code execution (RCE) when executed. **CVE ID : CVE-2019-9491**		
typestack_class-validator_project					
typestack_class-validator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	7.5	In TypeStack class-validator 0.10.2, validate() input validation can be bypassed because certain internal attributes can be overwritten via a conflicting name. Even though there is an optional forbidUnknownValues parameter that can be used to reduce the risk of this bypass, this option is not documented and thus most developers configure input validation in the vulnerable default manner. With this vulnerability, attackers can launch SQL Injection or XSS attacks by injecting arbitrary malicious input. NOTE: a software maintainer agrees with the "is not documented" finding but suggests that much of the responsibility for the risk lies in a different product. **CVE ID : CVE-2019-18413**	N/A	A-TYP-TYPE-041119/692
universal_office_converter_project					
universal_office_converter					

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-2019-17400**	N/A	A-UNI-UNIV-041119/693
url_redirect_project					
url_redirect					
Improper Neutralization 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/typo3-ext-sa-2019-015/	A-URL-URL_-041119/694
verodin					
director					
Improper Neutralization 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
Insufficiently 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	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10716		
video_converter_project					
video_converter					
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-VIDE-041119/697
Videolan					
vlc_media_player					
Improper Restriction of Operations within the Bounds of a Memory Buffer	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_license__3_0_0f+0x000000000 03b9aba. **CVE ID : CVE-2019-18278**	N/A	A-VID-VLC_-041119/698
Vmware					
cloud_foundation					
Incorrect Default Permissions	18-10-2019	5	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://www.vmware.com/security/advisories/VMSA-2019-0016.html	A-VMW-CLOU-041119/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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_container_registry					
Incorrect Default Permissions	18-10-2019	5	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 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**	http://www.vmware.com/security/advisories/VMSA-2019-0016.html	A-VMW-HARB-041119/700
wacom					
driver					
Improper Privilege Management	24-10-2019	7.2	An exploitable privilege escalation vulnerability exists in the Wacom, driver version 6.3.32-3,	N/A	A-WAC-DRIV-041119/701

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 Management	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/advisories/cve-	A-WHA-WHAT-041119/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**	2019-11933	
Wikidsystems					
2fa_enterprise_server					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-10-2019	6.5	A SQL injection vulnerability in processPref.jsp in WiKID 2FA Enterprise Server through 4.2.0-b2053 allows an authenticated user to execute arbitrary SQL commands via the processPref.jsp key parameter. **CVE ID : CVE-2019-17117**	N/A	A-WIK-2FA_-041119/704
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-2FA_-041119/705
two_factor_authentication_enterprise_server					
Improper	17-10-2019	6.5	WiKID Enterprise 2FA	N/A	A-WIK-TWO_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			(two factor 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 Neutralization 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 allows remote attackers to inject arbitrary web script or HTML via /WiKIDAdmin/userPreregistration.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-2019-17114**	N/A	A-WIK-TWO_-041119/707
Improper Neutralization of Input	17-10-2019	4.3	Multiple cross-site scripting (XSS) vulnerabilities in WiKID	N/A	A-WIK-TWO_-041119/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			2FA Enterprise Server through 4.2.0-b2047 allow remote attackers to inject arbitrary web script or 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.wikidsystems.server.GetDomainHash (2) S parameter to: - /wikid/DomainData - /wikid/PreRegisterLookup - /wikid/PreRegister - /wikid/InitDevice - /wikid/servlet/InitDevice2S - /wikid/servlet/InitDevice3S - /servlet/com.wikidsystems.server.InitDevice2S - /servlet/com.wikidsystems.server.InitDevice3S - /servlet/com.wikidsystems.server.InitDevice4S - /wikid/servlet/com.wikidsystems.server.InitDevice4AES - /wikid/servlet/com.wikidsystems.server.InitDevice5AES (3) a parameter to: - /wikid/PreRegisterLookup - /wikid/InitDevice - /wikid/servlet/InitDevice2S -		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/wikid/servlet/InitDevice3S - /servlet/com.wikidsystems.server.InitDevice2S - /servlet/com.wikidsystems.server.InitDevice3S - /servlet/com.wikidsystems.server.InitDevice4S - /wikid/servlet/com.wikidsystems.server.InitDevice4AES - /wikid/servlet/com.wikidsystems.server.InitDevice5AES. **CVE ID : CVE-2019-17115**		
Improper Neutralization 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-2019-17116**	N/A	A-WIK-TWO_-041119/709
Improper Neutralizati	17-10-2019	6.5	Multiple SQL injection vulnerabilities in Logs.jsp	N/A	A-WIK-TWO_-041119/710

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 Neutralization 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.jsp. 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.jsp 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

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 Neutralization 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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			(cross-site scripting) via the Customizer. **CVE ID : CVE-2019-17674**		041119/717
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. **CVE ID : CVE-2019-17675**	N/A	A-WOR-WORD-041119/718
wp-events-plugin					
events_manager					
Improper Neutralization 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-WP--EVEN-041119/719
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-041119/720

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_language_server_project					
xml_server_project					
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-2019-18212**	https://github.com/angelozerr/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/LSPXMLParserConfiguratio	https://github.com/angelozerr/lsp4xml/blob/master/CHANGELOG.md#others	A-XML-XML_-041119/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			n.java. **CVE ID : CVE-2019-18213**		
Xmlsoft					
libxslt					
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	A-XML-LIBX-041119/723
xnat					
xnat					
Improper Restriction of XML External Entity Reference ('XXE')	23-10-2019	4	WUSTL XNAT 1.7.5.3 allows XXE attacks via a POST request body. **CVE ID : CVE-2019-14276**	N/A	A-XNA-XNAT-041119/724
yalehome					
yale_bluetooth_key					
Improper Authentication	16-10-2019	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-YALE-041119/725

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 Neutralization 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 Neutralization 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 Neutralization 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 Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Neutralization 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-YOU-YOUP-041119/730
Improper Neutralization 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.json.php	N/A	A-YOU-YOUP-041119/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5121		
Improper Neutralization 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.json.php. **CVE ID : CVE-2019-5122**	N/A	A-YOU-YOUP-041119/732
Improper Neutralization 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.json.php. **CVE ID : CVE-2019-5123**	N/A	A-YOU-YOUP-041119/733
youphptube_encoder					
Improper Neutralization 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/getImage.php is vulnerable to a command	N/A	A-YOU-YOUP-041119/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection attack. **CVE ID : CVE-2019-5127**		
Improper Neutralization 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/getImageMP4.php is vulnerable to a command injection attack. **CVE ID : CVE-2019-5128**	N/A	A-YOU-YOUP-041119/735
Improper Neutralization 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/getSpiritsFromVideo.php is vulnerable to a command injection attack. **CVE ID : CVE-2019-5129**	N/A	A-YOU-YOUP-041119/736
zenspider					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ruby_parser-legacy					
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/legacy/ruby_parser.rb file. **CVE ID : CVE-2019-18409**	N/A	A-ZEN-RUBY-041119/737
Operating System					
Apple					
mac_os					
Improper Privilege Management	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	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-MAC_-041119/739
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-2019-8161**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/740
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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, 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**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/746

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/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/ap	O-APP-MAC_-041119/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			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**	sb19-49.html	
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-2019-8171**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/750
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/751

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
			CVE ID : CVE-2019-8172		
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/752
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**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/753
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/754

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/produc	O-APP-MAC_-041119/757

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/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/759

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 . **CVE ID : CVE-2019-8181**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/762

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/764
Out-of-	17-10-2019	10	Adobe Acrobat and Reader	https://helpx.	O-APP-MAC_-

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/767

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/770

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8193		
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/773
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 . **CVE ID : CVE-2019-8195**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/774
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-8196**		
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 . **CVE ID : CVE-2019-8197**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/776
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/777
Out-of-bounds Write	17-10-2019	7.5	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier,	https://helpx.adobe.com/security/produc	O-APP-MAC_-041119/778

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/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/780

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
			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, 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/security/products/acrobat/apsb19-49.html	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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/783

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 . **CVE ID : CVE-2019-8205**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/785
Out-of-	17-10-2019	5	Adobe Acrobat and Reader	https://helpx.	O-APP-MAC_-

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/788

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, 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/security/products/acrobat/apsb19-49.html	O-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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/791

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8214		
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-2019-8215**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/794
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-2019-8216**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/795
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/796

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/produc	O-APP-MAC_-041119/799

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/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/801

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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/804

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, 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. **CVE ID : CVE-2019-8226**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/805
Improper Privilege Management	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2019-8237**		
mac_os_x					
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/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/808
Improper Neutralization 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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-APP-MAC_-041119/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			2015.006.30503 and earlier have a cross-site scripting vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-8160**		
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-APP-MAC_-041119/810
Asus					
rog_zephyrus_m_gm501gs_firmware					
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	O-ASU-ROG_-041119/811

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_firmware					
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_firmware					
Allocation of Resources Without	17-10-2019	4.9	An issue was discovered in Bitdefender BOX firmware versions before 2.1.37.37-	N/A	O-BIT-BOX_-041119/813

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					
ubuntu_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 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.php?id=78599, https://support.f5.com/csp/article/K75408500?utm_source=f5support&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://security.netapp.com/advisory/ntap-20191017-0003/, https://support.f5.com/csp/article/K53746212?utm_s	O-CAN-UBUN-041119/815

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=f5support&utm_medium=RSS, https://www.sudo.ws/alerts/minus_1_uid.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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			ead_data in archive_read_support_format_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**		041119/818
Cisco					
250_series_firmware					
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 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 the targeted user. If the user has administrative privileges, the attacker could alter the	N/A	O-CIS-250_-041119/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration, execute commands, or cause a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2019-12636**		
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	O-CIS-250_-041119/820
350_series_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 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 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	O-CIS-350_-041119/821
Improper Neutralization 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	O-CIS-350_-041119/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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	N/A	O-CIS-550X-041119/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	O-CIS-550X-041119/824

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 browser-based information. **CVE ID : CVE-2019-12718**		
200_series_firmware					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based information. **CVE ID : CVE-2019-12718**		
300_series_firmware					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	O-CIS-300_-041119/826
aironet_1540_firmware					
Improper Privilege Managemen	16-10-2019	10	A vulnerability in Cisco Aironet Access Points (APs) Software could	N/A	O-CIS-AIRO-041119/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			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**		
Uncontrolled Resource Consumption	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	N/A	O-CIS-AIRO-041119/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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-AIRO-041119/829

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_1560_firmware					
Improper Privilege Management	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

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**		
Uncontrolled Resource Consumption	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	Patch	NCIIPC ID
			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-2019-15265**	N/A	O-CIS-AIRO-041119/832
aironet_1800_firmware					
Improper Privilege Management	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	N/A	O-CIS-AIRO-041119/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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-AIRO-041119/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_2800_firmware					
Improper Privilege Management	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	N/A	O-CIS-AIRO-041119/835

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. **CVE ID : CVE-2019-15260**		
Uncontrolled Resource Consumption	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.	N/A	O-CIS-AIRO-041119/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-15265**	N/A	O-CIS-AIRO-041119/837
aironet_3800_firmware					
Improper Privilege Management	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	N/A	O-CIS-AIRO-041119/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Uncontrolled Resource Consumption	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	N/A	O-CIS-AIRO-041119/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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	N/A	O-CIS-AIRO-041119/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) attack because an AP port could go offline. **CVE ID : CVE-2019-15265**		
aironet_4800_firmware					
Improper Privilege Management	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.	N/A	O-CIS-AIRO-041119/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15260		
Uncontrolled Resource Consumption	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	O-CIS-AIRO-041119/842
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	O-CIS-AIRO-041119/843

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. **CVE ID : CVE-2019-15261**		
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

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. **CVE ID : CVE-2019-15261**		
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

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. **CVE ID : CVE-2019-15261**		
Uncontrolled Resource Consumption	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	N/A	O-CIS-AIRO-041119/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
5500_wireless_controllers_firmware					
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	N/A	O-CIS-5500-041119/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, which could result in a DoS condition. **CVE ID : CVE-2019-15262**		
catalyst_9100_firmware					
Uncontrolled Resource Consumption	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	N/A	O-CIS-CATA-041119/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
firepower_management_center_2600_firmware					
Improper Neutralization 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-041119/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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-041119/850
firepower_appliance_7030_firmware					
Improper Neutralization 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-041119/851

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-2019-15268**		
Improper Neutralization 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-FIRE-041119/852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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_appliance_7110_firmware					
Improper Neutralization 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-FIRE-041119/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15268		
Improper Neutralization 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-041119/854
firepower_appliance_7115_firmware					
Improper Neutralization 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	O-CIS-FIRE-041119/855

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-2019-15268**		
Improper Neutralization 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-FIRE-041119/856

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**		
firepower_management_center_virtual_appliance_firmware					
Improper Neutralization 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	O-CIS-FIRE-041119/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15268		
Improper Neutralization 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-041119/858
firepower_management_center_2000_firmware					
Improper Neutralization 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-FIRE-041119/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			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**		
Improper Neutralization 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	O-CIS-FIRE-041119/860

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_management_center_1000_firmware					
Improper Neutralization 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	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2019-15268**		
Improper Neutralization 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-041119/862
firesight_management_center_3500_firmware					
Improper Neutralization of Input During Web Page Generation	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an	N/A	O-CIS-FIRE-041119/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('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-2019-15268**		
Improper Neutralization 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	O-CIS-FIRE-041119/864

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_appliance_7125_firmware					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2019-15268**		
Improper Neutralization 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-041119/866
firepower_management_center_4000_firmware					
Improper Neutralization 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-041119/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			(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**		
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/868

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**		
firepower_appliance_8290_firmware					
Improper Neutralization 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	Description & CVE ID	Patch	NCIIPC ID
			interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15268**		
Improper Neutralization 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-041119/870
firesight_management_center_1500_firmware					
Improper Neutralization of Input During Web	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower	N/A	O-CIS-FIRE-041119/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			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**		
Improper Neutralization 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-FIRE-041119/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
firesight_management_center_750_firmware					
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/873

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 Neutralization 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_appliance_7120_firmware					
Improper Neutralization of Input	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of	N/A	O-CIS-FIRE-041119/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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**		
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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-2019-15269**		
firepower_appliance_7010_firmware					
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15268**		
Improper Neutralization 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-041119/878
firepower_appliance_8370_firmware					
Improper Neutralizati	16-10-2019	3.5	Multiple vulnerabilities in the web-based	N/A	O-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			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**		041119/879
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_management_center_1600_firmware					
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/881

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 Neutralization 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
firepower_appliance_7020_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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-041119/883
Improper Neutralization 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-FIRE-041119/884

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**		
amp_8150_firmware					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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-2019-15268**		
Improper Neutralization 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-AMP_-041119/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firepower_appliance_8130_firmware					
Improper Neutralization 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 Neutralization 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-041119/888

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**		
spa122_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the web-based 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	2.9	A vulnerability in the web-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. 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**	N/A	O-CIS-SPA1-041119/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 files on an affected device. The vulnerability is due to improper input validation in 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 retrieve the contents of arbitrary files on the device, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2019-12704**	N/A	O-CIS-SPA1-041119/891
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 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-SPA1-041119/892

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-2019-15241**	N/A	O-CIS-SPA1-041119/894
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-15242**		
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	N/A	O-CIS-SPA1-041119/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2019-15244**	N/A	O-CIS-SPA1-041119/897
Improper Restriction of Operations	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could	N/A	O-CIS-SPA1-041119/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			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-2019-15245**		
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	O-CIS-SPA1-041119/899

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

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-2019-15248**	N/A	O-CIS-SPA1-041119/901
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	O-CIS-SPA1-041119/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-15249**		
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	N/A	O-CIS-SPA1-041119/903

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	O-CIS-SPA1-041119/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			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-2019-15252**		
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 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-SPA1-041119/906

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 web-based 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_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the web-based 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 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**	N/A	O-CIS-SPA1-041119/908
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 files on an affected device. The vulnerability is due to improper input validation in the web-based management interface. An	N/A	O-CIS-SPA1-041119/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	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 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 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-SPA1-041119/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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	O-CIS-SPA1-041119/911
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	N/A	O-CIS-SPA1-041119/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-15241**		
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 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.	N/A	O-CIS-SPA1-041119/913

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-2019-15244**		
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	N/A	O-CIS-SPA1-041119/916

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-2019-15245**		
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-2019-15246**	N/A	O-CIS-SPA1-041119/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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	O-CIS-SPA1-041119/918
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	N/A	O-CIS-SPA1-041119/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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.	N/A	O-CIS-SPA1-041119/920

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-2019-15251**		
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	N/A	O-CIS-SPA1-041119/923

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 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 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	O-CIS-SPA1-041119/925

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_firmware					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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-NGIP-041119/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
firepower_appliance_8390_firmware					
Improper Neutralization 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-041119/928
Improper Neutralization 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-041119/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			(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_appliance_8270_firmware					
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
Improper Neutralization 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-041119/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
firepower_management_center_4500_firmware					
Improper Neutralization 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-041119/932
Improper Neutralization of Input During Web	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower	N/A	O-CIS-FIRE-041119/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			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**		
firepower_appliance_8250_firmware					
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/935

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-2019-15269**		
firepower_management_center_4600_firmware					
Improper Neutralization 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-041119/936
Improper Neutralization of Input	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of	N/A	O-CIS-FIRE-041119/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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**		
firepower_management_center_2500_firmware					
Improper Neutralization 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	O-CIS-FIRE-041119/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	O-CIS-FIRE-041119/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
firepower_appliance_8120_firmware					
Improper Neutralization 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-041119/940
Improper Neutralizati	16-10-2019	3.5	Multiple vulnerabilities in the web-based	N/A	O-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			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**		041119/941
amp_7150_firmware					
Improper Neutralization 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-AMP_-041119/942

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-2019-15268**		
Improper Neutralization 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	N/A	O-CIS-AMP_-041119/943

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-2019-15269**		
firepower_appliance_8350_firmware					
Improper Neutralization 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 Neutralization 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-041119/945
firepower_appliance_8140_firmware					
Improper Neutralization 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

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-2019-15268**		
Improper Neutralization 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-FIRE-041119/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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_appliance_7050_firmware					
Improper Neutralization 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-FIRE-041119/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15268		
Improper Neutralization 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-041119/949
firepower_appliance_8260_firmware					
Improper Neutralization 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	O-CIS-FIRE-041119/950

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-2019-15268**		
Improper Neutralization 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-FIRE-041119/951

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**		
firepower_appliance_8360_firmware					
Improper Neutralization 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	O-CIS-FIRE-041119/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15268		
Improper Neutralization 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-041119/953
firepower_management_center_firmware					
Improper Neutralization 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-FIRE-041119/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			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 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_firmware					
Improper Neutralization 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	O-CIS-500_-041119/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Citrix					
application_delivery_controller_firmware					
Improper Authentication	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-APPL-041119/956
gateway_firmware					
Improper Authenticati	21-10-2019	7.5	An issue was discovered in Citrix Application Delivery	N/A	O-CIT-GATE-041119/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	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_gateway_firmware					
Improper Authentication	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-NETS-041119/958
clonos					
clonos					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Session Fixation	24-10-2019	7.5	clonos.php in ClonOS WEB control panel 19.09 allows remote attackers to gain full access via change password requests because there is no session management. **CVE ID : CVE-2019-18418**	N/A	O-CLO-CLON-041119/959
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-10-2019	4.3	A cross-site scripting (XSS) vulnerability in index.php in ClonOS WEB control panel 19.09 allows remote attackers to inject arbitrary web script or HTML via the lang parameter. **CVE ID : CVE-2019-18419**	N/A	O-CLO-CLON-041119/960
comtechefdata					
h8_heights_remote_gateway_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-10-2019	3.5	Comtech H8 Heights Remote Gateway 2.5.1 devices allow XSS and HTML injection via the Site Name (aka SiteName) field. **CVE ID : CVE-2019-17667**	N/A	O-COM-H8_H-041119/961
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://bugs.php.net/bug.php?id=78599, https://support.f5.com/csp/article/K75408500?utm_s	O-DEB-DEBI-041119/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	ource=f5support&utm_medium=RSS	
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L). **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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2983**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE product of Oracle Java	https://security.netapp.com	O-DEB-DEBI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in 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 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-2019-2987**	/advisory/ntap-20191017-0001/	041119/969
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE	https://security.netapp.com/advisory/nta	O-DEB-DEBI-041119/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	p-20191017-0001/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2988		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/971

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://security.netapp.com/advisory/ntap-20191017-0003/, https://support.f5.com/csp/article/K53746212?utm_source=f5support&utm_medium=RSS, https://www.sudo.ws/alerts/minus_1_uid.html	O-DEB-DEBI-041119/972
Interpretation 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://github.com/golang/go/issues/34960, https://groups.google.com/d/msg/golang-announce/lVEm7llp0w0/VbafyRkgCgAJ	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

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_read_data in archive_read_support_format_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**	N/A	O-DEB-DEBI-041119/975
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://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/978

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 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**		
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://security.netapp.com/advisory/ntap-20191017-0001/	O-DEB-DEBI-041119/979

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					
dir-412_firmware					
Improper Authentication	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	O-DLI-DIR--041119/980

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_firmware					
Improper Neutralization 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_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-EQ--HOME-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-EQ--HOME-041119/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can easily execute code and compromise the system. **CVE ID : CVE-2019-15850**		
ccu2_firmware					
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	O-EQ--CCU2-041119/984
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. **CVE ID : CVE-2019-14424**	N/A	O-EQ--CCU2-041119/985
Fedoraproject					
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://security.netapp.com/advisory/ntap-20191017-0003/, https://support.f5.com/csp	O-FED-FEDO-041119/986

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/K53746212?utm_source=f5support&utm_medium=RSS, https://www.sudo.ws/alerts/minus_1_uid.html	
hinet					
gpon_firmware					
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**	https://tvn.twcert.org.tw/taiwanvn/TVN-201908005, https://www.twcert.org.tw/en/cp-128-3013-92adb-2.html	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**	https://tvn.twcert.org.tw/taiwanvn/TVN-201908006, https://www.twcert.org.tw/en/cp-128-3014-904b1-2.html	O-HIN-GPON-041119/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	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.twcert.org.tw/taiwanvn/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.twcert.org.tw/taiwanvn/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 < I040GWR190731. 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-2019-15066**	https://tvn.twcert.org.tw/taiwanvn/TVN-201908012, https://www.twcert.org.tw/en/cp-128-3017-fd6bc-2.html	O-HIN-GPON-041119/991
Honeywell					
ip-ak2_firmware					
Missing	25-10-2019	5	In IP-AK2 Access Control	N/A	O-HON-IP-A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication 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
HP					
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**	N/A	O-HP-FUTU-041119/993
futuresmart_4					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. **CVE ID : CVE-2019-6334**	N/A	O-HP-FUTU-041119/994
inea					
me-rtu_firmware					
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	N/A	O-INE-ME-R-041119/995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 3.0. A world-readable /usr/smartrtu/init/settings.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**		
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, /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_dsa_key files that are publicly available from the vendor web sites. **CVE ID : CVE-2019-14926**	N/A	O-INE-ME-R-041119/996
Information	28-10-2019	5	An issue was discovered	N/A	O-INE-ME-R-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			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-2019-14927**		041119/997
Improper Neutralization 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-INE-ME-R-041119/998
Insufficiently 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-ME-R-041119/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 password due to insecure entries in /etc/sudoers on the RTU.) **CVE ID : CVE-2019-14930**	N/A	O-INE-ME-R-041119/1000
Improper Neutralization 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-ME-R-041119/1001

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://supportcontent.ibm.com/support/pages/node/1073236	O-LIN-LINU-041119/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4523		
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	O-LIN-LINU-041119/1003
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-10-2019	8.3	rtl_p2p_noa_ie in drivers/net/wireless/realtek/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-LINU-041119/1004
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	N/A	O-LIN-LINU-041119/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be disclosed. **CVE ID : CVE-2019-18197**		
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-LIN-LINU-041119/1006
Use After Free	24-10-2019	5	archive_read_format_rar_read_data in archive_read_support_format_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**	N/A	O-LIN-LINU-041119/1007
mi					
millet_router_3g_firmware					
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	N/A	O-MI-MILL-041119/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
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 authentication. **CVE ID : CVE-2019-18371**	N/A	O-MI-MILL-041119/1009
Microsoft					
windows					
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	https://supportcontent.ibm.com/support/pages/node/1073236	O-MIC-WIND-041119/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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	O-MIC-WIND-041119/1011
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-WIND-041119/1012

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://community.teamviewer.com/t5/Announcements/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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			nse__3_0_0f+0x00000000 03b9aba. **CVE ID : CVE-2019-18278**		
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/security/products/acrobat/apsb19-49.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/security/products/adm/apsb19-51.html	O-MIC-WIND-041119/1016
Improper Neutralization 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/security/products/acrobat/apsb19-49.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 . **CVE ID : CVE-2019-8161**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1018
Concurrent Execution using Shared Resource with Improper Synchronization ('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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1020

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1022
Improper	17-10-2019	6.8	Adobe Acrobat and Reader	https://helpx.	O-MIC-WIND-

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1025

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
			Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-8168**		
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://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1026
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 . **CVE ID : CVE-2019-8170**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1027
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1028

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8173		
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**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1031
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-2019-8175**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1032
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1033

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/produc	O-MIC-WIND-041119/1036

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/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1038

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 . **CVE ID : CVE-2019-8182**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1041

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1043
Use After	17-10-2019	4.3	Adobe Acrobat and Reader	https://helpx.	O-MIC-WIND-

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-8189**		
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1047
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-2019-8191**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1048
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1049

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8194		
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 . **CVE ID : CVE-2019-8195**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1052
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 . **CVE ID : CVE-2019-8196**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1053
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1054

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/produc	O-MIC-WIND-041119/1057

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/apsb19-49.html	
Out-of-bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier, 2017.011.30148 and earlier, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1059

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, 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/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30503 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-8205**		
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 . **CVE ID : CVE-2019-8206**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1063
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1064
Use After	17-10-2019	6.8	Adobe Acrobat and Reader	https://helpx.	O-MIC-WIND-

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-8210**		
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1068
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-2019-8212**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1069
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1070

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 . **CVE ID : CVE-2019-8214**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8215		
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-2019-8216**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1073
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1074
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	https://helpx.adobe.com/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1075

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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.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/security/produc	O-MIC-WIND-041119/1078

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-2019-8221**	ts/acrobat/apsb19-49.html	
Out-of-bounds Read	17-10-2019	5	Adobe Acrobat and Reader versions , 2019.012.20040 and earlier, 2017.011.30148 and earlier, 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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1079
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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1080

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 . **CVE ID : CVE-2019-8224**	https://helpx.adobe.com/security/products/acrobat/apsb19-49.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, 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/security/products/acrobat/apsb19-49.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/security/products/acrobat/apsb19-49.html	O-MIC-WIND-041119/1083

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 Management	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-MIC-WIND-041119/1084
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
Mitsubishielectric					
smartrtu_firmware					
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			readable /usr/smartrtu/init/settings.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**		
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 , /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_dsa_key files that are publicly available from the vendor web sites. **CVE ID : CVE-2019-14926**	N/A	O-MIT-SMAR-041119/1089
Information Exposure	28-10-2019	5	An issue was discovered on Mitsubishi Electric ME-	N/A	O-MIT-SMAR-041119/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-14927**		
Improper Neutralization 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-SMAR-041119/1091
Insufficiently 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-SMAR-041119/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 password due to insecure entries in /etc/sudoers on the RTU.) **CVE ID : CVE-2019-14930**	N/A	O-MIT-SMAR-041119/1093
Improper Neutralization of Special Elements used in an OS	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	N/A	O-MIT-SMAR-041119/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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_data_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-CLUS-041119/1095
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	https://supportcontent.ibm.com/support/	O-OPE-UNIX-041119/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			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. **CVE ID : CVE-2019-4523**	pages/node/1073236	
Opensuse					
leap					
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://security.netapp.com/advisory/ntap-20191017-0003/, https://support.f5.com/csp/article/K53746212?utm_source=f5support&utm_medium=RSS, https://www.sudo.ws/alerts/minus_1_uid.html	O-OPE-LEAP-041119/1097
Oracle					
solaris					
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	O-ORA-SOLA-041119/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data as well as unauthorized read access to a subset of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2019-2765**		
N/A	16-10-2019	1.2	Vulnerability in the Oracle Solaris product of Oracle Systems (component: LDAP Library). The supported version that is affected is 11. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle	N/A	O-ORA-SOLA-041119/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Solaris. 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 Oracle Solaris. CVSS 3.0 Base Score 1.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-3008**		
N/A	16-10-2019	4.6	Vulnerability in the Oracle Solaris product of Oracle Systems (component: XScreenSaver). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:	N/A	O-ORA-SOLA-041119/1100

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
			L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-3010**		
N/A	16-10-2019	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: SMF services & legacy daemons). The supported version that is affected is 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 3.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2019-2961**	N/A	O-ORA-SOLA-041119/1101
Redhat					
enterprise_linux_desktop					
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://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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/UI:R/S:U/C:N/I:N/A:L).		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2945		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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),	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1106

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 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 access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments,	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2987**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 Edition. While the vulnerability is in Oracle GraalVM Enterprise	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1111

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 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: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2999**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2962**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported	https://security.netapp.com/advisory/ntap-20191017-	O-RED-ENTE-041119/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	0001/	
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:	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2973**		
N/A	16-10-2019	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting).	https://security.netapp.com/advisory/ntap-20191017-	O-RED-ENTE-041119/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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	0001/	

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_linux_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://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 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,	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (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	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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2983**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in 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 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-2019-2987**		
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:	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
N/A	16-10-2019	4.3	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component:	https://security.netapp.com/advisory/ntap-20191017-	O-RED-ENTE-041119/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	0001/	
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2992**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1125

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
			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:		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2999**		
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 can also be exploited by using APIs in the specified Component, e.g., through a web service which	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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).	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
enterprise_linux_workstation					
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2945**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). 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 Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE,	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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: (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	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:	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2978**		
N/A	16-10-2019	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP).	https://security.netapp.com/advisory/ntap-20191017-	O-RED-ENTE-041119/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). 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**	0001/	

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
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://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1134

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-2019-2983**		
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 access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in 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 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://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 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**	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1137

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://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 ID : CVE-2019-2999**		
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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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,	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 some of Java SE, Java SE	https://security.netapp.com/advisory/ntap-20191017-0001/	O-RED-ENTE-041119/1143

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**		
Ricoh					
mp_501_firmware					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			drsSetUserWizard.cgi. **CVE ID : CVE-2019-18203**		
Samsung					
galaxy_s10_firmware					
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-GALA-041119/1145
note_10_firmware					
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-NOTE-041119/1146
Sangoma					
session_border_controller_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-10-2019	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	O-SAN-SESS-041119/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/Webconfig.inc.php and /usr/local/sng/bin/sng-user-mgmt. **CVE ID : CVE-2019-12147**		
Improper Authentication	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/Webconfig.inc.php. **CVE ID : CVE-2019-12148**	N/A	O-SAN-SESS-041119/1148
terra-master					
f2-210_firmware					
Improper Privilege Management	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-**	N/A	O-TER-F2-2-041119/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18195		
fs-210_firmware					
Information Exposure Through Log Files	23-10-2019	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?Event= substring. **CVE ID : CVE-2019-18385**	N/A	O-TER-FS-2-041119/1150
Tp-link					
m7350_firmware					
Improper Neutralization 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 externalPort OS Command Injection (issue 1 of 5). **CVE ID : CVE-2019-13649**	N/A	O-TP--M735-041119/1151
Improper Neutralization 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 internalPort OS Command Injection (issue 2 of 5). **CVE ID : CVE-2019-13650**	N/A	O-TP--M735-041119/1152
Improper Neutralization of Special Elements used in an	24-10-2019	10	TP-Link M7350 devices through 1.0.16 Build 181220 Rel.1116n allow portMappingProtocol OS Command Injection (issue	N/A	O-TP--M735-041119/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			3 of 5). **CVE ID : CVE-2019-13651**		
Improper Neutralization 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-TP--M735-041119/1154
Improper Neutralization 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-TP--M735-041119/1155
Wago					
pfc200_firmware					
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	O-WAG-PFC2-041119/1156
pfc100_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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	O-WAG-PFC1-041119/1157
Hardware					
Asus					
rog_zephyrus_m_gm501gs					
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 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."	N/A	H-ASU-ROG_-041119/1158

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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
webex_board_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_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	Description & CVE ID	Patch	NCIIPC ID
			15962		
webex_board_70					
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-041119/1163
webex_board_70s					
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.	N/A	H-CIS-WEBE-041119/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15962		
webex_board_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. **CVE ID : CVE-2019-15962**		
webex_room_55_dual					
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-041119/1167
webex_room_70_dual					
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	N/A	H-CIS-WEBE-041119/1168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/root directory of an affected device. **CVE ID : CVE-2019-15962**		
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-WEBE-041119/1169
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	N/A	H-CIS-WEBE-041119/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and writing files to the /root directory of an affected device. **CVE ID : CVE-2019-15962**		
webex_room_70_single_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-WEBE-041119/1171
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	N/A	H-CIS-WEBE-041119/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as the remotesupport user and writing files to the /root directory of an affected device. **CVE ID : CVE-2019-15962**		
firepower_management_center_1000					
Improper Neutralization 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-041119/1173
Improper Neutralization of Input	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of	N/A	H-CIS-FIRE-041119/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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**		
Improper Neutralization 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-FIRE-041119/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
firepower_management_center_2000					
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15268**		
Improper Neutralization 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-041119/1177
Improper Neutralization of Input	16-10-2019	3.5	A vulnerability in the web-based management interface of Cisco	N/A	H-CIS-FIRE-041119/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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 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**		
firepower_management_center_2500					
Improper Neutralization 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-FIRE-041119/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
Improper Neutralization 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 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**	N/A	H-CIS-FIRE-041119/1181
firepower_management_center_4000					
Improper Neutralizati	16-10-2019	3.5	Multiple vulnerabilities in the web-based	N/A	H-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			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**		041119/1182
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Neutralization 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 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	N/A	H-CIS-FIRE-041119/1184

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-2019-15270**		
firesight_management_center_1500					
Improper Neutralization 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-041119/1185
Improper Neutralization of Input	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of	N/A	H-CIS-FIRE-041119/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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**		
firesight_management_center_3500					
Improper Neutralization 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-FIRE-041119/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
firesight_management_center_750					
Improper Neutralization 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-041119/1189
Improper Neutralizati	16-10-2019	3.5	Multiple vulnerabilities in the web-based	N/A	H-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			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**		041119/1190
sf250-24					
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-SF25-041119/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF25-041119/1192

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 browser-based information. **CVE ID : CVE-2019-12718**		
sf250-24p					
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 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 the targeted user. If the	N/A	H-CIS-SF25-041119/1193

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF25-041119/1196

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 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**		
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF25-041119/1198

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg250-08					
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 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 the targeted user. If the	N/A	H-CIS-SG25-041119/1199

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG25-041119/1202

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 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**		
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG25-041119/1204

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg250-18					
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 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 the targeted user. If the	N/A	H-CIS-SG25-041119/1205

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG25-041119/1208

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 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**		
sg250-26hp					
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-SG25-041119/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG25-041119/1210

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg250-26p					
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 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 the targeted user. If the	N/A	H-CIS-SG25-041119/1211

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 Neutralization 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-based information. **CVE ID : CVE-2019-**	N/A	H-CIS-SG25-041119/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg250-50					
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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG25-041119/1214

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 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**		
sg250-50hp					
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-SG25-041119/1215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG25-041119/1216

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg250-50p					
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 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 the targeted user. If the	N/A	H-CIS-SG25-041119/1217

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG25-041119/1220

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 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**		
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-SG25-041119/1221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG25-041119/1222

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg250x-48					
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 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 the targeted user. If the	N/A	H-CIS-SG25-041119/1223

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG25-041119/1226

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 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**		
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF35-041119/1228

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 browser-based information. **CVE ID : CVE-2019-12718**		
sf350-24					
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 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 the targeted user. If the	N/A	H-CIS-SF35-041119/1229

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF35-041119/1232

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 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**		
sf350-24p					
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-SF35-041119/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF35-041119/1234

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 browser-based information. **CVE ID : CVE-2019-12718**		
sf350-48					
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 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 the targeted user. If the	N/A	H-CIS-SF35-041119/1235

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF35-041119/1238

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 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**		
sf350-48p					
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-SF35-041119/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF35-041119/1240

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 browser-based information. **CVE ID : CVE-2019-12718**		
sf352-08					
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 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 the targeted user. If the	N/A	H-CIS-SF35-041119/1241

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 Neutralization 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-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					
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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF35-041119/1244

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 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**		
sf352-08p					
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-SF35-041119/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF35-041119/1246

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg350-10					
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 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 the targeted user. If the	N/A	H-CIS-SG35-041119/1247

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG35-041119/1250

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 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**		
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-SG35-041119/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG35-041119/1252

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg350-10sfp					
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 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 the targeted user. If the	N/A	H-CIS-SG35-041119/1253

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG35-041119/1256

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 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**		
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG35-041119/1258

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg350-28mp					
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 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 the targeted user. If the	N/A	H-CIS-SG35-041119/1259

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG35-041119/1262

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 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**		
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-SG35-041119/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG35-041119/1264

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg350-52					
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 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 the targeted user. If the	N/A	H-CIS-SG35-041119/1265

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG35-041119/1268

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 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**		
sg350-52p					
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-SG35-041119/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SG35-041119/1270

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg350-8pd					
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 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 the targeted user. If the	N/A	H-CIS-SG35-041119/1271

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG35-041119/1274

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 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**		
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF55-041119/1276

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 browser-based information. **CVE ID : CVE-2019-12718**		
sf550x-24mp					
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 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 the targeted user. If the	N/A	H-CIS-SF55-041119/1277

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF55-041119/1280

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 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**		
sf550x-48					
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-SF55-041119/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SF55-041119/1282

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 browser-based information. **CVE ID : CVE-2019-12718**		
sf550x-48mp					
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 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 the targeted user. If the	N/A	H-CIS-SF55-041119/1283

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 Neutralization 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-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 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 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 Neutralization of Input	16-10-2019	4.3	A vulnerability in the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF55-041119/1286

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 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**		
spa122					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the web-based 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	2.9	A vulnerability in the web-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. 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	N/A	H-CIS-SPA1-041119/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2019-12703**		
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 files on an affected device. The vulnerability is due to improper input validation in 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 retrieve the contents of arbitrary files on the device, possibly resulting in the disclosure of sensitive information. **CVE ID : CVE-2019-12704**	N/A	H-CIS-SPA1-041119/1289
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	N/A	H-CIS-SPA1-041119/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	N/A	H-CIS-SPA1-041119/1291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with elevated privileges. Note: The web-based management interface is enabled by default. **CVE ID : CVE-2019-15240**		
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-2019-15241**	N/A	H-CIS-SPA1-041119/1292
Improper Restriction of Operations	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone Adapters (ATAs) could	N/A	H-CIS-SPA1-041119/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			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-2019-15242**		
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-	N/A	H-CIS-SPA1-041119/1294

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

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-2019-15245**	N/A	H-CIS-SPA1-041119/1296
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-SPA1-041119/1297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-15246**		
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	N/A	H-CIS-SPA1-041119/1298

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-2019-15247**		
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-2019-15248**	N/A	H-CIS-SPA1-041119/1299
Improper Restriction of	16-10-2019	5.2	Multiple vulnerabilities in Cisco SPA100 Series Analog Telephone	N/A	H-CIS-SPA1-041119/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			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-2019-15249**		
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	N/A	H-CIS-SPA1-041119/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enabled by default. **CVE ID : CVE-2019-15251**		
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-2019-15252**	N/A	H-CIS-SPA1-041119/1303
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-SPA1-041119/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Input Validation	16-10-2019	6.8	A vulnerability in the web-based 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,	N/A	H-CIS-SPA1-041119/1305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requiring manual intervention for recovery. **CVE ID : CVE-2019-15258**		
sf200-24					
Improper Neutralization 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-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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 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**		
sf200-24p					
Improper Neutralization 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	N/A	H-CIS-SF20-041119/1308

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**		
sf200-48					
Improper Neutralization 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	N/A	H-CIS-SF20-041119/1309

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 browser-based information. **CVE ID : CVE-2019-12718**		
sf200-48p					
Improper Neutralization 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	N/A	H-CIS-SF20-041119/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive browser-based information. **CVE ID : CVE-2019-12718**		
sf200e-24					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF20-041119/1311
sf200e-24p					
Improper	16-10-2019	4.3	A vulnerability in the web-	N/A	H-CIS-SF20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization 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 Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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					
Improper Neutralization 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-SF20-041119/1314

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 browser-based information. **CVE ID : CVE-2019-12718**		
sg200-08					
Improper Neutralization 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	N/A	H-CIS-SG20-041119/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2019-12718**		
sg200-08p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG20-041119/1316
sg200-10fp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG20-041119/1317
sg200-18					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg200-26					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg200-26fp					
Improper Neutralization 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	N/A	H-CIS-SG20-041119/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2019-12718**		
sg200-26p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG20-041119/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-50					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG20-041119/1322
sg200-50fp					
Improper Neutralization 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-SG20-041119/1323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		
sg200-50p					
Improper Neutralization 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-SG20-041119/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf300-08					
Improper Neutralization 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-SF30-041119/1325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf300-24					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF30-041119/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf300-24mp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF30-041119/1327
sf300-24p					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		
sf300-24pp					
Improper Neutralization 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-SF30-041119/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf300-48					
Improper Neutralization 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-SF30-041119/1330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf300-48p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF30-041119/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf300-48pp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF30-041119/1332
sf302-08					
Improper Neutralization 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-SF30-041119/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		
sf302-08mp					
Improper Neutralization 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-SF30-041119/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf302-08mpp					
Improper Neutralization 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-SF30-041119/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf302-08p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF30-041119/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf302-08pp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF30-041119/1337
sg300-10					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Neutralization 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-SG30-041119/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg300-10mpp					
Improper Neutralization 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-SG30-041119/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg300-10p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG30-041119/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-10pp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG30-041119/1342
sg300-10sfp					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		
sg300-20					
Improper Neutralization 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-SG30-041119/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg300-28					
Improper Neutralization 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-SG30-041119/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg300-28mp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG30-041119/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-28p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG30-041119/1347
amp_7150					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			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**		
Improper Neutralization 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-AMP_-041119/1349

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 Neutralization 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 Neutralization 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 Management	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Uncontrolled Resource Consumption	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	N/A	H-CIS-AIRO-041119/1353

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-2019-15264**		
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	N/A	H-CIS-AIRO-041119/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_1560					
Improper Privilege Management	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	N/A	H-CIS-AIRO-041119/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to disable the AP, creating a denial of service (DoS) condition for clients associated with the AP. **CVE ID : CVE-2019-15260**		
Uncontrolled Resource Consumption	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-AIRO-041119/1356
Improper Input	16-10-2019	2.1	A vulnerability in the bridge protocol data unit	N/A	H-CIS-AIRO-041119/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			(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-2019-15265**		
aironet_1800					
Improper Privilege Management	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-AIRO-041119/1358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Uncontrolled Resource Consumption	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-AIRO-041119/1359

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	Patch	NCIIPC ID
			15265		
aironet_2800					
Improper Privilege Management	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-AIRO-041119/1361
Uncontrolle	16-10-2019	6.1	A vulnerability in the	N/A	H-CIS-AIRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Resource Consumption			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**		041119/1362
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	N/A	H-CIS-AIRO-041119/1363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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 Management	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-AIRO-041119/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Uncontrolled Resource Consumption	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	N/A	H-CIS-AIRO-041119/1365

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 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**	N/A	H-CIS-AIRO-041119/1366
aironet_4800					
Improper Privilege Management	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Uncontrolled Resource Consumption	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	N/A	H-CIS-AIRO-041119/1368

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-2019-15264**		
aironet_1810					
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

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_1830					
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

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					
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-041119/1371

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**		
5508_wireless_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	N/A	H-CIS-5508-041119/1372

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_wireless_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which could result in a DoS condition. **CVE ID : CVE-2019-15262**		
catalyst_9100					
Uncontrolled Resource Consumption	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_management_center_2600					
Improper	16-10-2019	3.5	Multiple vulnerabilities in	N/A	H-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			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**		041119/1375
Improper Neutralization 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-FIRE-041119/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Neutralization 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 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	N/A	H-CIS-FIRE-041119/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15270**		
firepower_appliance_7030					
Improper Neutralization 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-041119/1378
Improper Neutralizati	16-10-2019	3.5	Multiple vulnerabilities in the web-based	N/A	H-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			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**		041119/1379
firepower_appliance_7110					
Improper Neutralization 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-FIRE-041119/1380

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-2019-15268**		
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1381

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-2019-15269**		
firepower_appliance_7115					
Improper Neutralization 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 Neutralization 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_management_center_virtual_appliance					
Improper Neutralization 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

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-2019-15268**		
Improper Neutralization 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-041119/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
Improper Neutralization 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 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**	N/A	H-CIS-FIRE-041119/1386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firepower_appliance_7125					
Improper Neutralization 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 Neutralization 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**		
firepower_appliance_8290					
Improper Neutralization 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

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 Neutralization 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 Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15269		
firepower_appliance_7120					
Improper Neutralization 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-041119/1391
Improper Neutralization 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-FIRE-041119/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			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_appliance_7010					
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1393

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-2019-15268**		
Improper Neutralization 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-041119/1394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2019-15269**		
firepower_appliance_8370					
Improper Neutralization 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-041119/1395
Improper Neutralization of Input During Web Page Generation	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an	N/A	H-CIS-FIRE-041119/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('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_management_center_1600					
Improper Neutralization 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-FIRE-041119/1397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	H-CIS-FIRE-041119/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
Improper Neutralization 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 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**	N/A	H-CIS-FIRE-041119/1399
firepower_appliance_7020					
Improper Neutralization 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-FIRE-041119/1400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			(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**		
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1401

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**		
firepower_appliance_8130					
Improper Neutralization 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	Description & CVE ID	Patch	NCIIPC ID
			interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15268**		
Improper Neutralization 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-041119/1403
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-SG55-041119/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			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 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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1405

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**		
sg550x-24mp					
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 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	N/A	H-CIS-SG55-041119/1406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2019-12718**		
sg550x-24mpp					
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 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 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	Description & CVE ID	Patch	NCIIPC ID
			device. **CVE ID : CVE-2019-12636**		
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG55-041119/1409
sg550x-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	N/A	H-CIS-SG55-041119/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg550x-48					
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 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	N/A	H-CIS-SG55-041119/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2019-12718**		
sg550x-48mp					
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 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 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.	N/A	H-CIS-SG55-041119/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-12636		
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG55-041119/1415
sg550x-48p					
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,	N/A	H-CIS-SG55-041119/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg550xg-24f					
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 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	N/A	H-CIS-SG55-041119/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive browser-based information. **CVE ID : CVE-2019-12718**		
sg550xg-24t					
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 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 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-SG55-041119/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12636		
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG55-041119/1421
sg550xg-48t					
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	N/A	H-CIS-SG55-041119/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg550xg-8f8t					
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 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	N/A	H-CIS-SG55-041119/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	N/A	H-CIS-SG55-041119/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access sensitive browser-based information. **CVE ID : CVE-2019-12718**		
sx550x-12f					
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 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 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-SX55-041119/1426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SX55-041119/1427
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-SX55-041119/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SX55-041119/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sx550x-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 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	N/A	H-CIS-SX55-041119/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	H-CIS-SX55-041119/1431

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 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 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	Patch	NCIIPC ID
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SX55-041119/1433
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-SX55-041119/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Neutralization 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-SX55-041119/1435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sx550x-52					
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 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	N/A	H-CIS-SX55-041119/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	H-CIS-SX55-041119/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based information. **CVE ID : CVE-2019-12718**		
spa112					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-10-2019	3.5	A vulnerability in the web-based 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 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**	N/A	H-CIS-SPA1-041119/1438
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	N/A	H-CIS-SPA1-041119/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files on an affected device. The vulnerability is due to improper input validation in 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 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 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 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	N/A	H-CIS-SPA1-041119/1440

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			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-2019-15241**		
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 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	N/A	H-CIS-SPA1-041119/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-15242**		
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	H-CIS-SPA1-041119/1444
Improper	16-10-2019	5.2	Multiple vulnerabilities in	N/A	H-CIS-SPA1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			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-2019-15244**		041119/1445
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	N/A	H-CIS-SPA1-041119/1446

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-2019-15245**		
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	N/A	H-CIS-SPA1-041119/1447

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			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-2019-15248**		
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 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	N/A	H-CIS-SPA1-041119/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-15249**		
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	H-CIS-SPA1-041119/1451
Improper	16-10-2019	5.2	Multiple vulnerabilities in	N/A	H-CIS-SPA1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			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**		041119/1452
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	N/A	H-CIS-SPA1-041119/1453

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 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 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15257		
Improper Input Validation	16-10-2019	6.8	A vulnerability in the web-based 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	H-CIS-SPA1-041119/1455
ngips_virtual_appliance					
Improper Neutralization 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	N/A	H-CIS-NGIP-041119/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
Improper Neutralization 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	N/A	H-CIS-NGIP-041119/1457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Neutralization 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 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**	N/A	H-CIS-NGIP-041119/1458
firepower_appliance_8390					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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-041119/1459
Improper Neutralization 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-FIRE-041119/1460

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_appliance_8270					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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-2019-15268**		
Improper Neutralization 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-041119/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firepower_management_center_4500					
Improper Neutralization 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 Neutralization 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	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 Neutralization 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 user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the	N/A	H-CIS-FIRE-041119/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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-2019-15270**		
firepower_appliance_8250					
Improper Neutralization 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	H-CIS-FIRE-041119/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15268		
Improper Neutralization 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-041119/1467
firepower_management_center_4600					
Improper Neutralization 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-FIRE-041119/1468

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-2019-15268**		
Improper Neutralization 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	H-CIS-FIRE-041119/1469

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 Neutralization 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 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	Description & CVE ID	Patch	NCIIPC ID
			15270		
firepower_appliance_8120					
Improper Neutralization 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-041119/1471
Improper Neutralization 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-FIRE-041119/1472

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-2019-15269**		
firepower_appliance_8350					
Improper Neutralization 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

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 Neutralization 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	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2019-15269**		
firepower_appliance_8140					
Improper Neutralization 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-041119/1475
Improper Neutralization of Input During Web Page Generation	16-10-2019	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an	N/A	H-CIS-FIRE-041119/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('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_appliance_7050					
Improper Neutralization 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-FIRE-041119/1477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Neutralization 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	H-CIS-FIRE-041119/1478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
firepower_appliance_8260					
Improper Neutralization 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-041119/1479
Improper Neutralization 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-FIRE-041119/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			(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_appliance_8360					
Improper Neutralization 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	N/A	H-CIS-FIRE-041119/1481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
Improper Neutralization 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-041119/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface or access sensitive, browser-based information. **CVE ID : CVE-2019-15269**		
firepower_management_center					
Improper Neutralization 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 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**	N/A	H-CIS-FIRE-041119/1483
webex_room_kit_mini					
Incorrect Default	16-10-2019	6.6	A vulnerability in the CLI of Cisco TelePresence	N/A	H-CIS-WEBE-041119/1484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			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**		
sg300-28pp					
Improper Neutralization 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	N/A	H-CIS-SG30-041119/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg300-28sfp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-**	N/A	H-CIS-SG30-041119/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg300-52					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG30-041119/1487
sg300-52mp					
Improper Neutralization 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-SG30-041119/1488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
sg300-52p					
Improper Neutralization 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-SG30-041119/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf500-24					
Improper Neutralization 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	N/A	H-CIS-SF50-041119/1490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf500-24mp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-**	N/A	H-CIS-SF50-041119/1491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sf500-24p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SF50-041119/1492
sf500-48					
Improper Neutralization 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-SF50-041119/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
sf500-48mp					
Improper Neutralization 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-SF50-041119/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sf500-48p					
Improper Neutralization 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	N/A	H-CIS-SF50-041119/1495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg500-28					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-**	N/A	H-CIS-SG50-041119/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg500-28mpp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG50-041119/1497
sg500-28p					
Improper Neutralization 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-SG50-041119/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
sg500-28pp					
Improper Neutralization 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-SG50-041119/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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					
Improper Neutralization 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	N/A	H-CIS-SG50-041119/1500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg500-52mp					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-**	N/A	H-CIS-SG50-041119/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg500-52p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG50-041119/1502
sg500-52pp					
Improper Neutralization 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-SG50-041119/1503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
sg500x-24					
Improper Neutralization 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-SG50-041119/1504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg500x-24mpp					
Improper Neutralization 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	N/A	H-CIS-SG50-041119/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
sg500x-24p					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-**	N/A	H-CIS-SG50-041119/1506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12718		
sg500x-48					
Improper Neutralization 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-based information. **CVE ID : CVE-2019-12718**	N/A	H-CIS-SG50-041119/1507
sg500x-48mpp					
Improper Neutralization 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-SG50-041119/1508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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**		
sg500x-48p					
Improper Neutralization 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-SG50-041119/1509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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					
Improper Neutralization 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	N/A	H-CIS-SG50-041119/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Citrix					
netscaler_gateway					
Improper Authentication	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	H-CIT-NETS-041119/1511
application_delivery_controller					
Improper Authentication	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	N/A	H-CIT-APPL-041119/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
gateway					
Improper Authentication	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	H-CIT-GATE-041119/1513
comtechefdata					
h8_heights_remote_gateway					
Improper Neutralization of Input During Web Page Generation	17-10-2019	3.5	Comtech H8 Heights Remote Gateway 2.5.1 devices allow XSS and HTML injection via the Site Name (aka SiteName) field.	N/A	H-COM-H8_H-041119/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2019-17667**		
Dlink					
dir-412					
Improper Authentication	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 act=clear&logtype=sysact to log_clear.php, which could be used to erase attack traces. **CVE ID : CVE-2019-17512**	N/A	H-DLI-DIR--041119/1515
dir-866l					
Improper Neutralization 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	H-DLI-DIR--041119/1516
eq-3					
homematic_ccu3					
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	N/A	H-EQ--HOME-041119/1517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could create SSH logins after a valid session and easily compromise the system. **CVE ID : CVE-2019-15849**		
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 can easily execute code and compromise the system. **CVE ID : CVE-2019-15850**	N/A	H-EQ--HOME-041119/1518
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-EQ--CCU2-041119/1519
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-EQ--CCU2-041119/1520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-14424		
hinet					
gpon					
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**	https://tvn.twcert.org.tw/taiwanvn/TVN-201908005, https://www.twcert.org.tw/en/cp-128-3013-92adb-2.html	H-HIN-GPON-041119/1521
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**	https://tvn.twcert.org.tw/taiwanvn/TVN-201908006, https://www.twcert.org.tw/en/cp-128-3014-904b1-2.html	H-HIN-GPON-041119/1522
Improper Authentication	17-10-2019	7.5	HiNet GPON firmware version < I040GWR190731 allows an attacker login to device without any authentication. **CVE ID : CVE-2019-**	https://tvn.twcert.org.tw/taiwanvn/TVN-201908007, https://www.twcert.org.tw/en/cp-128-3015-170fe-	H-HIN-GPON-041119/1523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15064	2.html	
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.twcert.org.tw/taiwanvn/TVN-201908011, https://www.twcert.org.tw/en/cp-128-3016-b0e90-2.html	H-HIN-GPON-041119/1524
Improper Input Validation	17-10-2019	10	An ?invalid command? handler issue was discovered in HiNet GPON firmware < I040GWR190731. 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-2019-15066**	https://tvn.twcert.org.tw/taiwanvn/TVN-201908012, https://www.twcert.org.tw/en/cp-128-3017-fd6bc-2.html	H-HIN-GPON-041119/1525
Honeywell					
ip-ak2					
Missing Authentication 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-IP-A-041119/1526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over the network. **CVE ID : CVE-2019-13525**		
HP					
laserjet_enterprise_m653_j8a06a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1527
laserjet_managed_e65050_l3u55a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1528
laserjet_managed_e65050_l3u56a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1529
laserjet_managed_e65050_l3u57a					
Improper Input	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and	N/A	H-HP-LASE-041119/1530

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_managed_e65060_l3u55a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_e65060_l3u56a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_e65060_l3u57a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
laserjet_enterprise_m750_d3l08a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1534
laserjet_enterprise_m750_d3l09a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1535
laserjet_enterprise_m750_d3l10a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1536
laserjet_enterprise_m751_t3u43a					
Improper Input Validation	16-10-2019	7.5	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-041119/1537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_m751_t3u44a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1538
laserjet_enterprise_m751_t3u64a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1539
laserjet_managed_e75245_t3u43a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1540
laserjet_managed_e75245_t3u44a					
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-041119/1541

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_managed_e75245_t3u64a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m855_a2w77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m855_a2w78a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m855_a2w79a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1545
laserjet_enterprise_m855_d7p72a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1546
laserjet_enterprise_m855_d7p73a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1547
laserjet_enterprise_flow_mfp_m577_b5l46a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
laserjet_enterprise_flow_mfp_m577_b5l47a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1549
laserjet_enterprise_flow_mfp_m577_b5l48a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1550
laserjet_enterprise_flow_mfp_m577_b5l54a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1551
laserjet_enterprise_mfp_m577_b5l46a					
Improper Input Validation	16-10-2019	7.5	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-041119/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_mfp_m577_b5l47a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1553
laserjet_enterprise_mfp_m577_b5l48a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_mfp_m577_b5l54a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_flow_mfp_m577_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

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_managed_flow_mfp_m577_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_managed_mfp_m577_b5l49a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_m577_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-041119/1559
laserjet_enterprise_flow_mfp_m680_ca251a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1560
laserjet_enterprise_flow_mfp_m680_cz248a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1561
laserjet_enterprise_flow_mfp_m680_cz249a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1562
laserjet_enterprise_flow_mfp_m680_cz250a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1563

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
laserjet_enterprise_mfp_m680_ca251a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1564
laserjet_enterprise_mfp_m680_cz248a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1565
laserjet_enterprise_mfp_m680_cz249a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1566
laserjet_enterprise_mfp_m680_cz250a					
Improper Input Validation	16-10-2019	7.5	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-041119/1567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_m680_l3u47a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1568
laserjet_managed_flow_mfp_m680_l3u48a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1569
laserjet_managed_mfp_m680_l3u47a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1570
laserjet_managed_mfp_m680_l3u48a					
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-041119/1571

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_enterprise_flow_mfp_m681_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_enterprise_flow_mfp_m681_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_enterprise_flow_mfp_m681_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_enterprise_flow_mfp_m681_j8a13a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1575
laserjet_enterprise_flow_mfp_m682_j8a16a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1576
laserjet_enterprise_flow_mfp_m682_j8a17a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1577
laserjet_enterprise_mfp_m681_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-041119/1578

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
laserjet_enterprise_mfp_m681_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-041119/1579
laserjet_enterprise_mfp_m681_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-041119/1580
laserjet_enterprise_mfp_m681_j8a13a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1581
laserjet_enterprise_mfp_m682_j8a16a					
Improper Input Validation	16-10-2019	7.5	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-041119/1582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_mfp_m682_j8a17a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1583
laserjet_managed_flow_mfp_e67550_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_managed_flow_mfp_e67550_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_managed_flow_mfp_e67550_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

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_managed_flow_mfp_e67550_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_managed_flow_mfp_e67560_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_enterprises_cp5525_ce709a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_e55040dw_3gx98a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1590
laserjet_managed_flow_mfp_e77822_x3a77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1591
laserjet_managed_mfp_e77825_z8z00a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1592
laserjet_managed_mfp_e77825_z8z02a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1593

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
laserjet_managed_mfp_e77825_z8z04a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77830_x3a78a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_managed_mfp_e77830_x3a81a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1596
laserjet_managed_mfp_e77830_x3a84a					
Improper Input Validation	16-10-2019	7.5	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e87640_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1598
laserjet_managed_flow_mfp_e87640_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_managed_flow_mfp_e87640_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_managed_flow_mfp_e87640_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

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_managed_flow_mfp_e87640_z8z12a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_flow_mfp_e87640_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_managed_flow_mfp_e87640_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_managed_flow_mfp_e87640_z8z15a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1605
laserjet_managed_flow_mfp_e87640_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-041119/1606
laserjet_managed_flow_mfp_e87640_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-041119/1607
laserjet_managed_flow_mfp_e87650_x3a86a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1608

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
laserjet_managed_flow_mfp_e87650_x3a87a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1609
laserjet_managed_flow_mfp_e87650_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1610
laserjet_managed_flow_mfp_e87650_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-041119/1611
laserjet_managed_flow_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	N/A	H-HP-LASE-041119/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e87650_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-041119/1613
laserjet_managed_flow_mfp_e87650_z8z12a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1614
laserjet_managed_flow_mfp_e87650_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-041119/1615
laserjet_managed_flow_mfp_e87650_z8z14a					
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-041119/1616

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_managed_flow_mfp_e87650_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_managed_flow_mfp_e87650_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_managed_flow_mfp_e87650_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_managed_flow_mfp_e87660_x3a86a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1620
laserjet_managed_flow_mfp_e87660_x3a87a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1621
laserjet_managed_flow_mfp_e87660_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1622
laserjet_managed_flow_mfp_e87660_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-041119/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
laserjet_managed_flow_mfp_e87660_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_managed_flow_mfp_e87660_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
laserjet_managed_flow_mfp_e87660_z8z12a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1626
laserjet_managed_flow_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	N/A	H-HP-LASE-041119/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e87660_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-041119/1628
laserjet_managed_flow_mfp_e87660_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-041119/1629
laserjet_managed_flow_mfp_e87660_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-041119/1630
laserjet_managed_flow_mfp_e87660_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-LASE-041119/1631

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_managed_mfp_e87640_x3a86a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1632
laserjet_managed_mfp_e87640_x3a87a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1633
laserjet_managed_mfp_e87640_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1634
laserjet_managed_mfp_e87640_x3a90a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1635
laserjet_managed_mfp_e87640_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-041119/1636
laserjet_managed_mfp_e87640_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-041119/1637
laserjet_managed_mfp_e87640_z8z12a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1638

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
laserjet_managed_mfp_e87640_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-041119/1639
laserjet_managed_mfp_e87640_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-041119/1640
laserjet_managed_mfp_e87640_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-041119/1641
laserjet_managed_mfp_e87640_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	N/A	H-HP-LASE-041119/1642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e87640_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-041119/1643
laserjet_managed_mfp_e87650_x3a86a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1644
laserjet_managed_mfp_e87650_x3a87a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1645
laserjet_managed_mfp_e87650_x3a89a					
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-041119/1646

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_managed_mfp_e87650_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-041119/1647
laserjet_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_managed_mfp_e87650_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-041119/1649
laserjet_managed_mfp_e87650_z8z12a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1650
laserjet_managed_mfp_e87650_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-041119/1651
laserjet_managed_mfp_e87650_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-041119/1652
laserjet_managed_mfp_e87650_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-041119/1653

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
laserjet_managed_mfp_e87650_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-041119/1654
laserjet_managed_mfp_e87650_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-041119/1655
laserjet_managed_mfp_e87660_x3a86a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1656
laserjet_managed_mfp_e87660_x3a87a					
Improper Input Validation	16-10-2019	7.5	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e87660_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1658
laserjet_managed_mfp_e87660_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-041119/1659
laserjet_managed_mfp_e87660_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-041119/1660
laserjet_managed_mfp_e87660_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-041119/1661

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_managed_mfp_e87660_z8z12a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_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_managed_mfp_e87660_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-041119/1664
laserjet_managed_mfp_e87660_z8z15a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1665
laserjet_managed_mfp_e87660_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-041119/1666
laserjet_managed_mfp_e87660_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-041119/1667
laserjet_enterprise_500_m551_cf081a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1668

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
laserjet_enterprise_500_m551_cf082a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_500_m551_cf083a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_500_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	H-HP-LASE-041119/1671
laserjet_enterprise_500_mfp_m575_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_500_mfp_m575_cd646a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1673
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	H-HP-LASE-041119/1674
laserjet_enterprise_flow_mfp_m575_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 code. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1675
laserjet_enterprise_flow_mfp_m575_cd646a					
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

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_managed_500_mfp_m575_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-041119/1677
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_managed_flow_mfp_m575_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_managed_flow_mfp_m575_l3u46a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1680
laserjet_enterprise_500_mfp_m525f_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1681
laserjet_managed_mfp_m725_cf068a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1682
laserjet_managed_mfp_m725_cf069a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1683

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
laserjet_managed_mfp_m725_l3u63a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1684
laserjet_managed_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-041119/1685
laserjet_managed_mfp_e72425_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-041119/1686
laserjet_managed_mfp_e72425_5cm69a					
Improper Input Validation	16-10-2019	7.5	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-041119/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e72425_5cm70a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1688
laserjet_managed_mfp_e72425_5cm71a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1689
laserjet_managed_mfp_e72425_5cm72a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1690
laserjet_managed_mfp_e72425_5rc89a					
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

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_managed_mfp_e72425_5rc90a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e72430_5cm69a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e72430_5cm70a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1695
laserjet_managed_mfp_e72430_5cm71a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1696
laserjet_managed_mfp_e72430_5cm72a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1697
laserjet_managed_mfp_e72430_5rc89a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1698

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
laserjet_managed_mfp_e72430_5rc90a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_flow_mfp_e72525_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
laserjet_managed_flow_mfp_e72525_x3a60a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1701
laserjet_managed_flow_mfp_e72525_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e72525_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-041119/1703
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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1704
laserjet_managed_flow_mfp_e72525_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_managed_flow_mfp_e72525_z8z010a					
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-041119/1706

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_managed_flow_mfp_e72525_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_managed_flow_mfp_e72525_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_managed_flow_mfp_e72525_z8z08a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1710
laserjet_managed_flow_mfp_e72525_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-041119/1711
laserjet_managed_flow_mfp_e72530_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-041119/1712
laserjet_managed_flow_mfp_e72530_x3a60a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1713

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
laserjet_managed_flow_mfp_e72530_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_managed_flow_mfp_e72530_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
laserjet_managed_flow_mfp_e72530_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1716
laserjet_managed_flow_mfp_e72530_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e72530_z8z010a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1718
laserjet_managed_flow_mfp_e72530_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-041119/1719
laserjet_managed_flow_mfp_e72530_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-041119/1720
laserjet_managed_flow_mfp_e72530_z8z07a					
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-041119/1721

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_managed_flow_mfp_e72530_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_managed_flow_mfp_e72530_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_managed_flow_mfp_e72535_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_managed_flow_mfp_e72535_x3a60a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1725
laserjet_managed_flow_mfp_e72535_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-041119/1726
laserjet_managed_flow_mfp_e72535_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-041119/1727
laserjet_managed_flow_mfp_e72535_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
laserjet_managed_flow_mfp_e72535_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-041119/1729
laserjet_managed_flow_mfp_e72535_z8z010a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1730
laserjet_managed_flow_mfp_e72535_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-041119/1731
laserjet_managed_flow_mfp_e72535_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	N/A	H-HP-LASE-041119/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e72535_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-041119/1733
laserjet_managed_flow_mfp_e72535_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-041119/1734
laserjet_managed_flow_mfp_e72535_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-041119/1735
laserjet_managed_mfp_e72525_x3a59a					
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-041119/1736

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_managed_mfp_e72525_x3a60a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e72525_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-041119/1738
laserjet_managed_mfp_e72525_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-041119/1739
laserjet_managed_mfp_e72525_x3a65a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1740
laserjet_managed_mfp_e72525_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-041119/1741
laserjet_managed_mfp_e72525_z8z010a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1742
laserjet_managed_mfp_e72525_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-041119/1743

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
laserjet_managed_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-041119/1744
laserjet_managed_mfp_e72525_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-041119/1745
laserjet_managed_mfp_e72525_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-041119/1746
laserjet_managed_mfp_e72525_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	N/A	H-HP-LASE-041119/1747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e72530_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-041119/1748
laserjet_managed_mfp_e72530_x3a60a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e72530_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-041119/1750
laserjet_managed_mfp_e72530_x3a63a					
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

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_managed_mfp_e72530_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1752
laserjet_managed_mfp_e72530_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-041119/1753
laserjet_managed_mfp_e72530_z8z010a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e72530_z8z011a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1755
laserjet_managed_mfp_e72530_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-041119/1756
laserjet_managed_flow_mfp_e77822_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-041119/1757
laserjet_managed_flow_mfp_e77822_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-041119/1758

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
laserjet_managed_mfp_e77825_x3a78a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1759
laserjet_managed_mfp_e77428_5rc91a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1760
laserjet_managed_flow_mfp_e77822_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-041119/1761
laserjet_managed_flow_mfp_e77822_z8z05a					
Improper Input Validation	16-10-2019	7.5	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-041119/1762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e77822_z8z0a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1763
laserjet_managed_flow_mfp_e77825_x3a77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1764
laserjet_managed_flow_mfp_e67560_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-041119/1765
laserjet_managed_flow_mfp_e67560_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-041119/1766

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_managed_flow_mfp_e67560_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	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e67550_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-041119/1769
laserjet_managed_mfp_e67550_l3u69a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1770
laserjet_managed_mfp_e67550_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-041119/1771
laserjet_managed_mfp_e67560_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-041119/1772
laserjet_managed_mfp_e67560_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-041119/1773

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
laserjet_managed_mfp_e67560_l3u69a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1774
laserjet_managed_mfp_e67560_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-041119/1775
laserjet_enterprises_cp5525_ce707a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1776
laserjet_enterprises_cp5525_ce708a					
Improper Input Validation	16-10-2019	7.5	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-041119/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e77825_x3a81a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1778
laserjet_managed_mfp_e77825_x3a84a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1779
laserjet_managed_flow_mfp_e87640_x3a86a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1780
laserjet_managed_flow_mfp_e87640_x3a87a					
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-041119/1781

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_managed_flow_mfp_e77825_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_managed_flow_mfp_e77825_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_managed_flow_mfp_e77825_z8z05a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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_managed_flow_mfp_e77825_z8z0a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1786
laserjet_managed_flow_mfp_e77830_x3a77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1787
laserjet_managed_flow_mfp_e77830_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-041119/1788

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
laserjet_managed_flow_mfp_e77830_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_managed_flow_mfp_e77830_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-041119/1790
laserjet_managed_flow_mfp_e77830_z8z05a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1791
laserjet_managed_mfp_e77830_z8z04a					
Improper Input Validation	16-10-2019	7.5	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e57540_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1793
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_managed_mfp_e57540_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1795
laserjet_managed_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	N/A	H-HP-LASE-041119/1796

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_managed_mfp_e77422_5cm75a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77422_5cm76a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_managed_mfp_e77422_5cm77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77422_5cm78a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1800
laserjet_managed_mfp_e77422_5rc91a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1801
laserjet_managed_mfp_e77422_5rc92a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1802
laserjet_managed_mfp_e77428_5cm75a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1803

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
laserjet_managed_mfp_e77428_5cm76a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1804
laserjet_managed_mfp_e77428_5rc92a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1805
laserjet_managed_flow_mfp_e77830_z8z0a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1806
laserjet_managed_mfp_e77822_x3a78a					
Improper Input Validation	16-10-2019	7.5	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-041119/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e77822_x3a81a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1808
laserjet_managed_mfp_e77822_x3a84a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77822_z8z00a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77822_z8z02a					
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

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_managed_mfp_e77822_z8z04a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77830_z8z00a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77830_z8z02a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e77422_5cm79a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1815
laserjet_managed_mfp_e77428_5cm77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1816
laserjet_managed_mfp_e77428_5cm78a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1817
laserjet_managed_mfp_e77428_5cm79a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1818

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
laserjet_managed_mfp_e72530_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-041119/1819
laserjet_managed_mfp_e72530_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-041119/1820
laserjet_managed_mfp_e72530_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-041119/1821
laserjet_managed_mfp_e72535_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	N/A	H-HP-LASE-041119/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e72535_x3a60a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1823
laserjet_managed_mfp_e72535_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-041119/1824
laserjet_managed_mfp_e72535_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-041119/1825
laserjet_managed_mfp_e72535_x3a65a					
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-041119/1826

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_managed_mfp_e72535_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-041119/1827
laserjet_managed_mfp_e72535_z8z010a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_managed_mfp_e72535_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-041119/1829
laserjet_managed_mfp_e72535_z8z06a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1830
laserjet_managed_mfp_e72535_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-041119/1831
laserjet_managed_mfp_e72535_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-041119/1832
laserjet_managed_mfp_e72535_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-041119/1833

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
laserjet_managed_flow_mfp_e82540_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_managed_flow_mfp_e82540_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
laserjet_managed_flow_mfp_e82540_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-041119/1836
laserjet_managed_flow_mfp_e82540_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e82540_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-041119/1838
laserjet_managed_flow_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_managed_flow_mfp_e82540_x3a75a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1840
laserjet_managed_flow_mfp_e82540_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

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_managed_flow_mfp_e82540_x3a82a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_flow_mfp_e82540_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_managed_flow_mfp_e82540_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_managed_flow_mfp_e82540_z8z22a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1845
laserjet_managed_flow_mfp_e82540_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-041119/1846
laserjet_managed_flow_mfp_e82550_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-041119/1847
laserjet_managed_flow_mfp_e82550_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-041119/1848

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
laserjet_managed_flow_mfp_e82550_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_managed_flow_mfp_e82550_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
laserjet_managed_flow_mfp_e82550_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-041119/1851
laserjet_managed_flow_mfp_e82550_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e82550_x3a75a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1853
laserjet_managed_flow_mfp_e82550_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 code. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1854
laserjet_managed_flow_mfp_e82550_x3a82a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1855
laserjet_managed_flow_mfp_e82550_z8z18a					
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-041119/1856

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_managed_flow_mfp_e82550_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-041119/1857
laserjet_managed_flow_mfp_e82550_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_managed_flow_mfp_e82550_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_managed_flow_mfp_e82560_az8z20a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1860
laserjet_managed_flow_mfp_e82560_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-041119/1861
laserjet_managed_flow_mfp_e82560_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-041119/1862
laserjet_managed_flow_mfp_e82560_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-041119/1863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
laserjet_managed_flow_mfp_e82560_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_managed_flow_mfp_e82560_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
laserjet_managed_flow_mfp_e82560_x3a75a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1866
laserjet_managed_flow_mfp_e82560_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e82560_x3a82a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1868
laserjet_managed_flow_mfp_e82560_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-041119/1869
laserjet_managed_flow_mfp_e82560_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-041119/1870
laserjet_managed_flow_mfp_e82560_z8z22a					
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-041119/1871

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_managed_flow_mfp_e82560_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-041119/1872
laserjet_managed_mfp_e82540_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-041119/1873
laserjet_managed_mfp_e82540_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-041119/1874
laserjet_managed_mfp_e82540_x3a69a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1875
laserjet_managed_mfp_e82540_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-041119/1876
laserjet_managed_mfp_e82540_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-041119/1877
laserjet_managed_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-041119/1878

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
laserjet_managed_mfp_e82540_x3a75a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e82540_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 code. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1880
laserjet_managed_mfp_e82540_x3a82a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1881
laserjet_managed_mfp_e82540_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	N/A	H-HP-LASE-041119/1882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e82540_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-041119/1883
laserjet_managed_mfp_e82540_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-041119/1884
laserjet_managed_mfp_e82540_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-041119/1885
laserjet_managed_mfp_e82550_az8z20a					
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-041119/1886

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_managed_mfp_e82550_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-041119/1887
laserjet_managed_mfp_e82550_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-041119/1888
laserjet_managed_mfp_e82550_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-041119/1889
laserjet_managed_mfp_e82550_x3a72a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1890
laserjet_managed_mfp_e82550_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-041119/1891
laserjet_managed_mfp_e82550_x3a75a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1892
laserjet_managed_mfp_e82550_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 code. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1893

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
laserjet_managed_mfp_e82550_x3a82a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e82550_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-041119/1895
laserjet_managed_mfp_e82550_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-041119/1896
laserjet_managed_mfp_e82550_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	N/A	H-HP-LASE-041119/1897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_e82550_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-041119/1898
laserjet_managed_mfp_e82560_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-041119/1899
laserjet_managed_mfp_e82560_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-041119/1900
laserjet_managed_mfp_e82560_x3a69a					
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-041119/1901

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_managed_mfp_e82560_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-041119/1902
laserjet_managed_mfp_e82560_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-041119/1903
laserjet_managed_mfp_e82560_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-041119/1904
laserjet_managed_mfp_e82560_x3a75a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1905
laserjet_managed_mfp_e82560_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 code. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1906
laserjet_managed_mfp_e82560_x3a82a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1907
laserjet_managed_mfp_e82560_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-041119/1908

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
laserjet_managed_mfp_e82560_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-041119/1909
laserjet_managed_mfp_e82560_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-041119/1910
laserjet_managed_mfp_e82560_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-041119/1911
officejet_enterprise_flow_mfp_x585_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	N/A	H-HP-OFFI-041119/1912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
officejet_enterprise_flow_mfp_x585_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-OFFI-041119/1913
officejet_enterprise_flow_mfp_x585_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_enterprise_mfp_x585_b5l04a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_mfp_x585_b5l05a					
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-OFFI-041119/1916

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_enterprise_mfp_x585_l3u40a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_flow_mfp_x585_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
officejet_managed_flow_mfp_x585_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-OFFI-041119/1919
officejet_managed_flow_mfp_x585_l3u41a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-OFFI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1920
officejet_managed_mfp_x585_b5l04a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1921
officejet_managed_mfp_x585_b5l05a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1922
officejet_managed_mfp_x585_l3u40a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1923

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
officejet_enterprise_x555_c2s11a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_x555_c2s12a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
officejet_enterprise_x555_l1h45a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1926
pagewide_755_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
pagewide_enterprise_765_j7z04a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1928
pagewide_managed_e75160_j7z06a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1929
pagewide_managed_p75250_y3z49a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1930
pagewide_managed_mfp_p77440_y3z60a					
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-PAGE-041119/1931

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_managed_mfp_p77940_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_managed_mfp_p77940_2gp23a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_p77940_2gp25a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_p77940_2gp26a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1935
pagewide_managed_mfp_p77940_5zn98a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1936
pagewide_managed_mfp_p77940_5zn99a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1937
pagewide_managed_mfp_p77940_5zp00a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1938

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
pagewide_managed_mfp_p77940_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_managed_mfp_p77940_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
pagewide_managed_mfp_p77940_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-041119/1941
pagewide_managed_mfp_p77940_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
pagewide_managed_mfp_p77940_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-PAGE-041119/1943
pagewide_managed_mfp_p77940_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-PAGE-041119/1944
pagewide_managed_mfp_p77940_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-PAGE-041119/1945
pagewide_managed_mfp_p77940_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-PAGE-041119/1946

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_managed_mfp_p77950_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_managed_mfp_p77950_2gp23a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_p77950_2gp25a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_p77950_2gp26a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1950
pagewide_managed_mfp_p77950_5zn98a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1951
pagewide_managed_mfp_p77950_5zn99a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1952
pagewide_managed_mfp_p77950_5zp00a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1953

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
pagewide_managed_mfp_p77950_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_managed_mfp_p77950_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
pagewide_managed_mfp_p77950_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-041119/1956
pagewide_managed_mfp_p77950_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
pagewide_managed_mfp_p77950_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-PAGE-041119/1958
pagewide_managed_mfp_p77950_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-PAGE-041119/1959
pagewide_managed_mfp_p77950_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-PAGE-041119/1960
pagewide_managed_mfp_p77950_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-PAGE-041119/1961

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_managed_mfp_p77960_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_managed_mfp_p77960_2gp23a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_p77960_2gp25a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_p77960_2gp26a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1965
pagewide_managed_mfp_p77960_5zn98a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1966
pagewide_managed_mfp_p77960_5zn99a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1967
pagewide_managed_mfp_p77960_5zp00a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1968

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
pagewide_managed_mfp_p77960_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_managed_mfp_p77960_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
laserjet_enterprise_500_mfp_m525f_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-041119/1971
laserjet_enterprise_500_mfp_m525f_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_flow_mfp_m525_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1973
laserjet_enterprise_flow_mfp_m525_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_enterprise_flow_mfp_m525_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 code. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/1975
laserjet_managed_500_mfp_m525_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

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_managed_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_managed_flow_mfp_m525_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_managed_flow_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-041119/1979
laserjet_enterprise_600_m601_ce989a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1980
laserjet_enterprise_600_m601_ce990a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1981
laserjet_enterprise_600_m602_ce991a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1982
laserjet_enterprise_600_m602_ce992a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1983

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
laserjet_enterprise_600_m602_ce993a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1984
laserjet_enterprise_600_m603_ce991a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_600_m603_ce992a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1986
laserjet_enterprise_600_m603_ce993a					
Improper Input Validation	16-10-2019	7.5	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-041119/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_700_mfp_m775_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
laserjet_enterprise_700_mfp_m775_cc523a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1989
laserjet_enterprise_700_mfp_m775_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_enterprise_700_mfp_m775_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

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_enterprise_700_mfp_m775_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_enterprise_700_mfp_m775_l3u50a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_m775_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-041119/1994
laserjet_managed_mfp_m775_cc523a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/1995
laserjet_managed_mfp_m775_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-041119/1996
laserjet_managed_mfp_m775_cf304a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1997
laserjet_managed_mfp_m775_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-041119/1998

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
laserjet_managed_mfp_m775_l3u50a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/1999
laserjet_enterprise_700_m712_cf235a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2000
laserjet_enterprise_700_m712_cf236a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2001
laserjet_enterprise_700_m712_cf238a					
Improper Input Validation	16-10-2019	7.5	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-041119/2002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_flow_mfp_m630_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/2003
laserjet_enterprise_flow_mfp_m630_l3u62a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_enterprise_flow_mfp_m630_p7z47a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_flow_mfp_m630_p7z48a					
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-041119/2006

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_enterprise_mfp_m630_b3g84a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_mfp_m630_b3g85a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_enterprise_mfp_m630_j7x28a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_mfp_m630_l3u61a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2010
laserjet_managed_flow_mfp_m630_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/2011
laserjet_managed_flow_mfp_m630_l3u62a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2012
laserjet_managed_flow_mfp_m630_p7z47a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2013

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
laserjet_managed_flow_mfp_m630_p7z48a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2014
laserjet_managed_mfp_m630_b3g84a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2015
laserjet_managed_mfp_m630_b3g85a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2016
laserjet_managed_mfp_m630_j7x28a					
Improper Input Validation	16-10-2019	7.5	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-041119/2017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_mfp_m630_l3u61a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2018
laserjet_enterprise_flow_mfp_m830_cf367a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2019
laserjet_enterprise_flow_mfp_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-041119/2020
laserjet_managed_flow_mfp_m830_cf367a					
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

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_managed_flow_mfp_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_enterprise_m4555_mfp_ce502a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m4555_mfp_ce503a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m4555_mfp_ce504a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2025
laserjet_enterprise_m4555_mfp_ce738a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2026
laserjet_enterprise_m506_f2a66a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2027
laserjet_enterprise_m506_f2a67a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2028

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
laserjet_enterprise_m506_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_enterprise_m506_f2a69a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_enterprise_m506_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
laserjet_enterprise_m506_f2a71a					
Improper Input Validation	16-10-2019	7.5	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-041119/2032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_m506_f2a66a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2033
laserjet_managed_m506_f2a67a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2034
laserjet_managed_m506_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-041119/2035
laserjet_managed_m506_f2a69a					
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-041119/2036

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_managed_m506_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-041119/2037
laserjet_managed_m506_f2a71a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m507_1pu51a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m507_1pu52a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2040
laserjet_enterprise_m507_1pv86a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2041
laserjet_enterprise_m507_1pv87a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2042
laserjet_enterprise_m507_1pv88a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2043

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
laserjet_enterprise_m507_1pv89a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2044
laserjet_managed_e50145_1pu51a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2045
laserjet_managed_e50145_1pu52a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2046
laserjet_managed_e50145_1pv86a					
Improper Input Validation	16-10-2019	7.5	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-041119/2047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_e50145_1pv87a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2048
laserjet_managed_e50145_1pv88a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2049
laserjet_managed_e50145_1pv89a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2050
laserjet_enterprise_m604_e6b67a					
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-041119/2051

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_enterprise_m604_e6b68a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2052
laserjet_enterprise_m605_e6b69a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2053
laserjet_enterprise_m605_e6b70a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2054
laserjet_enterprise_m605_e6b71a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2055
laserjet_enterprise_m605_l3u53a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2056
laserjet_enterprise_m605_l3u54a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2057
laserjet_enterprise_m606_e6b72a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2058

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
laserjet_enterprise_m606_e6b73a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2059
laserjet_managed_m605_e6b69a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2060
laserjet_managed_m605_e6b70a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2061
laserjet_managed_m605_e6b71a					
Improper Input Validation	16-10-2019	7.5	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-041119/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_m605_l3u53a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2063
laserjet_managed_m605_l3u54a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2064
laserjet_enterprise_m607_k0q14a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2065
laserjet_enterprise_m607_k0q15a					
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-041119/2066

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_enterprise_m608_k0q17a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m608_k0q18a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m608_k0q19a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m608_m0p32a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2070
laserjet_enterprise_m609_k0q20a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2071
laserjet_enterprise_m609_k0q21a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2072
laserjet_enterprise_m609_k0q22a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2073

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
laserjet_managed_e60075_m0p33a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2074
laserjet_managed_e60075_m0p35a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2075
laserjet_managed_e60075_m0p36a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2076
laserjet_managed_e60075_m0p39a					
Improper Input Validation	16-10-2019	7.5	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-041119/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_e60075_m0p40a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2078
laserjet_enterprise_m806_cz244a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2079
laserjet_enterprise_m806_cz245a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2080
laserjet_enterprise_flow_mfp_m527z_f2a76a					
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-041119/2081

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_enterprise_flow_mfp_m527z_f2a77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_flow_mfp_m527z_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_enterprise_flow_mfp_m527z_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_enterprise_mfp_m527_f2a76a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2085
laserjet_enterprise_mfp_m527_f2a77a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2086
laserjet_enterprise_mfp_m527_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-041119/2087
laserjet_enterprise_mfp_m527_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-041119/2088

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
laserjet_managed_flow_mfp_m527z_f2a79a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2089
laserjet_managed_flow_mfp_m527z_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-LASE-041119/2090
laserjet_managed_mfp_m527_f2a79a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2091
laserjet_managed_mfp_m527_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	N/A	H-HP-LASE-041119/2092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_mfp_m528_1ps54a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2093
laserjet_enterprise_mfp_m528_1ps55a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2094
laserjet_enterprise_mfp_m528_1pv49a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2095
laserjet_enterprise_mfp_m528_1pv64a					
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-041119/2096

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_enterprise_mfp_m528_1pv65a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_mfp_m528_1pv66a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_mfp_m528_1pv67a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_e52645_1ps54a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2100
laserjet_managed_mfp_e52645_1ps55a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2101
laserjet_managed_mfp_e52645_1pv49a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2102
laserjet_managed_mfp_e52645_1pv64a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2103

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
laserjet_managed_mfp_e52645_1pv65a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2104
laserjet_managed_mfp_e52645_1pv66a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2105
laserjet_managed_mfp_e52645_1pv67a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2106
laserjet_enterprise_flow_mfp_m631_j8j63a					
Improper Input Validation	16-10-2019	7.5	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-041119/2107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_flow_mfp_m631_j8j64a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2108
laserjet_enterprise_flow_mfp_m631_j8j65a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2109
laserjet_enterprise_flow_mfp_m632_j8j70a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2110
laserjet_enterprise_flow_mfp_m632_j8j71a					
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-041119/2111

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_enterprise_flow_mfp_m632_j8j72a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2112
laserjet_enterprise_flow_mfp_m633_j8j76a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2113
laserjet_enterprise_flow_mfp_m633_j8j78a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2114
laserjet_enterprise_mfp_m631_j8j63a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2115
laserjet_enterprise_mfp_m631_j8j64a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2116
laserjet_enterprise_mfp_m631_j8j65a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2117
laserjet_enterprise_mfp_m632_j8j70a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2118

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
laserjet_enterprise_mfp_m632_j8j71a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2119
laserjet_enterprise_mfp_m632_j8j72a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2120
laserjet_enterprise_mfp_m633_j8j76a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2121
laserjet_enterprise_mfp_m633_j8j78a					
Improper Input Validation	16-10-2019	7.5	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-041119/2122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e62555_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-041119/2123
laserjet_managed_flow_mfp_e62555_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_managed_flow_mfp_e62555_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_managed_flow_mfp_e62555_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

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_managed_flow_mfp_e62555_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	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_flow_mfp_e62565_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_managed_flow_mfp_e62565_j8j67a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2130
laserjet_managed_flow_mfp_e62565_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-041119/2131
laserjet_managed_flow_mfp_e62565_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/2132
laserjet_managed_flow_mfp_e62565_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-041119/2133

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
laserjet_managed_flow_mfp_e62565_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_managed_flow_mfp_e62575_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
laserjet_managed_flow_mfp_e62575_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-041119/2136
laserjet_managed_flow_mfp_e62575_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_flow_mfp_e62575_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/2138
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-LASE-041119/2139
laserjet_managed_flow_mfp_e62575_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-041119/2140
laserjet_managed_mfp_e62555_j8j66a					
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-041119/2141

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_managed_mfp_e62555_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-041119/2142
laserjet_managed_mfp_e62555_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-041119/2143
laserjet_managed_mfp_e62555_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/2144
laserjet_managed_mfp_e62555_j8j79a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2145
laserjet_managed_mfp_e62555_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-041119/2146
laserjet_managed_mfp_e62565_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-041119/2147
laserjet_managed_mfp_e62565_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-041119/2148

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
laserjet_managed_mfp_e62565_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-041119/2149
laserjet_managed_mfp_e62565_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-LASE-041119/2150
laserjet_managed_mfp_e62565_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-041119/2151
laserjet_managed_mfp_e62565_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	N/A	H-HP-LASE-041119/2152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_mfp_m725_cf066a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2153
laserjet_enterprise_mfp_m725_cf067a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2154
laserjet_enterprise_mfp_m725_cf068a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2155
laserjet_enterprise_mfp_m725_cf069a					
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-041119/2156

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_enterprise_mfp_m725_l3u63a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_m725_cf066a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_m725_cf067a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2160
laserjet_cm4540_mfp_cc419a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2161
laserjet_cm4540_mfp_cc420a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2162
laserjet_cm4540_mfp_cc421a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2163

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
laserjet_enterprise_flow_mfp_m880z_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_enterprise_flow_mfp_m880z_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
laserjet_enterprise_flow_mfp_m880z_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-041119/2166
laserjet_enterprise_flow_mfp_m880z_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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_enterprise_flow_mfp_m880z_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-041119/2168
laserjet_enterprise_flow_mfp_m880z_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_managed_flow_mfp_m880zm_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_managed_flow_mfp_m880zm_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

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_managed_flow_mfp_m880zm_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_managed_flow_mfp_m880zm_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_managed_flow_mfp_m880zm_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_managed_flow_mfp_m880zm_l3u52a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2175
laserjet_enterprise_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-LASE-041119/2176
laserjet_enterprise_m553_b5l24a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2177
laserjet_enterprise_m553_b5l25a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2178

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
laserjet_enterprise_m553_b5l26a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2179
laserjet_enterprise_m553_b5l38a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2180
laserjet_enterprise_m553_b5l39a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2181
laserjet_enterprise_m553_bl27a					
Improper Input Validation	16-10-2019	7.5	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-041119/2182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_m553_b5l24a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2183
laserjet_managed_m553_b5l25a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2184
laserjet_managed_m553_b5l26a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2185
laserjet_managed_m553_b5l38a					
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

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_managed_m553_b5l39a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_m553_bl27a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m651_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_enterprise_m651_cz256a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-LASE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		041119/2190
laserjet_enterprise_m651_cz257a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2191
laserjet_enterprise_m651_h0dc9a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2192
laserjet_enterprise_m651_l8z07a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2193

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
laserjet_managed_m651_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-041119/2194
laserjet_managed_m651_cz256a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_managed_m651_cz257a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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
laserjet_managed_m651_h0dc9a					
Improper Input Validation	16-10-2019	7.5	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
laserjet_managed_m651_l8z07a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-041119/2198
laserjet_enterprise_m652_j7z98a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m652_j7z99a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_m653_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

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_enterprise_m653_j8a05a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_mfp_p77960_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_managed_mfp_p77960_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_managed_mfp_p77960_y3z64a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		051119/2205
pagewide_managed_mfp_p77960_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-PAGE-051119/2206
pagewide_managed_mfp_p77960_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-PAGE-051119/2207
pagewide_managed_mfp_p77960_y3z68a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2208

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
pagewide_mfp_774_4pa44a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_mfp_774_4pz43a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_mfp_779_4pz45a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_mfp_779_4pz46a					
Improper Input Validation	16-10-2019	7.5	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
pagewide_enterprise_556_g1w46a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2213
pagewide_enterprise_556_g1w46v					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2214
pagewide_enterprise_556_g1w47a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2215
pagewide_enterprise_556_g1w47v					
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-PAGE-051119/2216

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_managed_e55650_l3u44a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_enterprise_flow_mfp_780f_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_enterprise_flow_mfp_780f_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_enterprise_flow_mfp_785_j7z11a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		051119/2220
pagewide_enterprise_flow_mfp_785_j7z12a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2221
pagewide_enterprise_mfp_780_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-051119/2222
pagewide_enterprise_mfp_780_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-051119/2223

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
pagewide_managed_flow_mfp_e77650_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_managed_flow_mfp_e77650_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
pagewide_managed_flow_mfp_e77650_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-051119/2226
pagewide_managed_flow_mfp_e77650_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	N/A	H-HP-PAGE-051119/2227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
pagewide_managed_flow_mfp_e77650_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-PAGE-051119/2228
pagewide_managed_flow_mfp_e77660z_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_managed_flow_mfp_e77660z_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-051119/2230
pagewide_managed_flow_mfp_e77660z_j7z07a					
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-PAGE-051119/2231

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_managed_flow_mfp_e77660z_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_managed_flow_mfp_e77660z_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_managed_flow_mfp_e77660z_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_managed_flow_mfp_e77660z_z5g77a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		051119/2235
pagewide_managed_flow_mfp_e77660z_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-PAGE-051119/2236
pagewide_managed_mfp_e77650_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-051119/2237
pagewide_managed_mfp_e77650_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-051119/2238

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
pagewide_managed_mfp_e77650_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_managed_mfp_e77650_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
pagewide_managed_mfp_e77650_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. **CVE ID : CVE-2019-6334**	N/A	H-HP-PAGE-051119/2241
pagewide_enterprise_flow_mfp_586z_g1w39a					
Improper Input Validation	16-10-2019	7.5	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **CVE ID : CVE-2019-6334**		
pagewide_enterprise_flow_mfp_586z_g1w40a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2243
pagewide_enterprise_flow_mfp_586z_g1w41a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2244
pagewide_enterprise_mfp_586_g1w39a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2245
pagewide_enterprise_mfp_586_g1w40a					
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-PAGE-051119/2246

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_enterprise_mfp_586_g1w41a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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_managed_flow_mfp_e58650z_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_managed_flow_mfp_e58650z_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_managed_mfp_e58650dn_l3u42a					
Improper	16-10-2019	7.5	HP LaserJet, PageWide,	N/A	H-HP-PAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**		051119/2250
pagewide_managed_mfp_e58650dn_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-051119/2251
scanjet_enterprise_8500_fn1_document_capture_workstation_l2717a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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-051119/2252
digital_sender_flow_8500_fn2_document_capture_workstation_l2762a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers have a solution to check application signature that may allow potential execution of arbitrary code. **CVE ID : CVE-2019-6334**	N/A	H-HP-DIGI-051119/2253

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
scanjet_enterprise_flow_n9120_fn2_document_scanner_l2763a					
Improper Input Validation	16-10-2019	7.5	HP LaserJet, PageWide, OfficeJet Enterprise, and LaserJet Managed Printers 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					
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/settings.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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 , /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_dsa_key files that are publicly available from the vendor web sites. **CVE ID : CVE-2019-14926**		
Information Exposure	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. 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-2019-14927**	N/A	H-INE-ME-R-051119/2257
Improper Neutralization 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	N/A	H-INE-ME-R-051119/2258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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-INE-ME-R-051119/2259
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	N/A	H-INE-ME-R-051119/2260

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 Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-14931		
mi					
millet_router_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**		
Mitsubishielectric					
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/settings.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	Patch	NCIIPC ID
			, /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_dsa_key files that are publicly available from the vendor web sites. **CVE ID : CVE-2019-14926**		
Information Exposure	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. 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-2019-14927**	N/A	H-MIT-SMAR-051119/2266
Improper Neutralization 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-**	N/A	H-MIT-SMAR-051119/2267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14928		
Insufficiently 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

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 Neutralization 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_5-051119/2271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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/adrsSetUserWizard.cgi. **CVE ID : CVE-2019-18203**		
Samsung					
galaxy_s10					
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	H-SAM-GALA-051119/2272
note_10					
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	H-SAM-NOTE-051119/2273
Sangoma					
session_border_controller					
Improper Neutralization 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-SESS-051119/2274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream 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/Webconfig.inc.php and /usr/local/sng/bin/sng-user-mgmt. **CVE ID : CVE-2019-12147**		
Improper Authentication	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/Webconfig.inc.php. **CVE ID : CVE-2019-12148**	N/A	H-SAN-SESS-051119/2275
terra-master					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
f2-210					
Improper Privilege Management	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-2019-18195**	N/A	H-TER-F2-2-051119/2276
fs-210					
Information Exposure Through Log Files	23-10-2019	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?Event= substring. **CVE ID : CVE-2019-18385**	N/A	H-TER-FS-2-051119/2277
Tp-link					
m7350					
Improper Neutralization 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 externalPort OS Command Injection (issue 1 of 5). **CVE ID : CVE-2019-13649**	N/A	H-TP--M735-051119/2278
Improper Neutralization of Special Elements used in an OS Command	24-10-2019	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	H-TP--M735-051119/2279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')					
Improper Neutralization 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-TP--M735-051119/2280
Improper Neutralization 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-TP--M735-051119/2281
Improper Neutralization 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-TP--M735-051119/2282
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

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. **CVE ID : CVE-2019-18202**		
pfc100					
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	H-WAG-PFC1-051119/2284