

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

16 - 31 Aug 2019

Vol. 06 No. 16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Application		
Acdsee					
photo_studi	0				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-08-2019	4.6	An issue was discovered in ACDSee Photo Studio Standard 22.1 Build 1159. There is a User Mode Write AV starting at IDE_ACDStd!IEP_ShowPlugInDial og+0x0000000000023d060. CVE ID: CVE-2019-15293	N/A	A-ACD- PHOT- 060919/1
Adobe					
acrobat_dc					
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7965	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/2
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/3
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . CVE ID: CVE-2019-8002		
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8003	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/4
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8004	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/5
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/6
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7 2	7-8	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8005		
NULL Pointer Dereferenc e	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8006	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/7
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8007	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/8
Out-of- bounds Write	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/9
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8	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-2019-8008		
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8009	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/10
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8010	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/11
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/12
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8011		
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8012	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/13
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8013	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/14
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-41.html		A-ADO- ACRO- 060919/15
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7 5	7-8	9-10

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID	
			earlier have vulnerabili exploitation arbitrary co	ty. Succe n could l ode exec	essful ead to ution .	N					
			CVE ID : CV								
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	7.5	versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8015				https://elpx.ad e.com/s urity/p ducts/a obat/ap 19- 41.htm	ob sec oro acr osb	A-A ACR 060		
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8016				https://elpx.ad e.com/s urity/p ducts/a obat/ap 19- 41.htm	ob sec oro acr osb	A-A ACR 060	-	
NULL Pointer Dereferenc e	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and				versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, 2015.006.30497 and elpx.adob e.com/sec urity/products/acr		ob sec oro acr osb	A-A ACR 060	
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-	.9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8017		
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8018	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/19
Incorrect Type Conversion or Cast	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8019	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/20
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/21
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID		
			rea exp info	lier have d vulner ploitation ormation E ID : CV	rability. n could l n disclos	Successfead to ure.							
Out-of- bounds Read	20-08-2019	5	Add ver ear ear ear ear ear ear rea exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8021 Adobe Acrobat and Reader					ro ecr	A-A ACR 060			
Out-of- bounds Write	20-08-2019	7.5	ver ear ear ear ear ear ear ear	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and				https://elpx.ade e.com/s urity/p ducts/a obat/ap 19- 41.htm	ob sec ro acr osb	A-A ACR 060	_		
Out-of- bounds Write	20-08-2019	7.5	ver ear ear ear ear	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and					versions, 2019.012.20035 and earlier, 2019.012.20035 and e.com/sec earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, 2015.006.30497 and elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-		ob sec ro acr osb	A-A ACR 060	
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-2019-8023		
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8024	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/25
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8025	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/26
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/27
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	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-2019-8026		
Out-of- bounds Write	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8027	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/28
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8028	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/29
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and elpx.adob earlier, 2019.012.20035 and e.com/sec earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and https://h elpx.adob elpx.adob elpx.adob e.com/sec urity/pro ducts/acr obat/apsb earlier, 2017.011.30142 and earlier, 2015.006.30498 and 41.html		A-ADO- ACRO- 060919/30
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Da	ite	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID			
				vul exp	nerabili loitatio	e an use ty. Succe n could l ode exec	ead to	е							
				CVI	E ID : CV	E-2019	-8029								
Use After Free	20-08-20	19	7.5	ver ear ear ear ear ear vul exp arb	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8030				https://elpx.ad e.com/urity/p ducts/a obat/aj 19- 41.htm	ob sec oro acr psb	A-A ACR 060				
				CVI	E ID : CV	E-2019	-8030								
Use After Free	20-08-20	19	7.5	ver ear ear ear ear ear vul exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8031				https://elpx.ad e.com// urity/p ducts/a obat/aj 19- 41.htm	ob sec oro acr psb	A-A ACR 060	-			
Out-of- bounds Read	20-08-20	19	5	ver ear ear ear ear	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and					versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, 2015.006.30497 and		https://elpx.ad e.com/urity/p ducts/a obat/ap 19- 41.htm	ob sec oro acr psb	A-A ACR 060	
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 read vulnerability. Successful exploitation could lead to information disclosure . CVE ID : CVE-2019-8032 Adobe Acrobat and Reader		
Use After Free	20-08-2019	6.8	versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8033	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/34
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8034	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/35
Out-of- bounds Read	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsh earlier, 2017.011.30142 and earlier, 2015.006.30498 and 41.html		A-ADO- ACRO- 060919/36
CV Scoring Scale (CVSS)	9 0-1 1-3	2 2	earlier, and 2015.006.30498 and -3		9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . CVE ID: CVE-2019-8035		
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8036	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/37
Out-of- bounds Read	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8037	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/38
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/39
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Dat	CVSS	Description & CVE ID					Patch	1	N	CIIPC ID
			vul exp arb	lier have nerabili ploitation pitrary co	ty. Succe n could l ode exec	essful ead to ution.	e				
Use After Free	20-08-201	9 6.8	Add ver ear ear ear ear ear vul exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8039					ro ecr	A-A ACR 060	
Out-of- bounds Read	20-08-201	9 4.3	ver ear ear ear ear ear rea exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8040				https://elpx.ad/e.com/surity/pducts/aobat/ap19-41.htm	ob sec ro acr osb	A-A ACR 060	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-201	9 7.5	ver ear ear ear ear	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and				versions, 2019.012.20035 and elpx.adob earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-		A-A ACR 060	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8041		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8042	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/43
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8043	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/44
Double Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/45
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	-9 9-10

Weakness	Publish Da	ate	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
				vul exp arb	nerabilit loitation itrary co	e a doub ty. Succe n could l ode exec /E-2019	essful ead to ution.					
NULL Pointer Dereferenc e	20-08-20	19	7.5	ver ear ear ear ear ear der Suc to a	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8045				https://elpx.ad e.com/s urity/p ducts/a obat/ap 19- 41.htm	ob sec oro acr osb	A-A ACR 060	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-20	19	7.5	ver ear ear ear ear ear vuli exp arb	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8046				https://elpx.ad e.com/s urity/p ducts/a obat/an 19- 41.htm	ob sec oro acr osb	A-A ACR 060	
Use After Free	20-08-20	19	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and				e.com/sec urity/pro ducts/acr obat/apsb 19-		0-		
CV Scoring Scale (CVSS)	0-1	1-2	2	3	3-4	4-5	5-6	6-7	7-8	8-	9	9-10

Weakness	Publish Da	ate	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
				vul exp	nerabili oloitatio	e an use ty. Succe n could l ode exec	ead to	e				
				CV	E ID : CV	/E-2019	-8047					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-20	019	7.5	ver ear ear ear ear ear vul exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8048					/h ob sec oro acr psb	A-A ACR 060	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-20	019	10	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8049					https://elpx.ad e.com/s urity/p ducts/a obat/an 19- 41.htm	ob sec oro acr psb	A-A ACR 060	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-20)19	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and					https://elpx.ad e.com/s urity/p ducts/a obat/ap 19- 41.htm	ob sec oro acr psb	A-A ACR 060	
CV Scoring Scale (CVSS)	0-1	1-2	2 2-3 3-4 4-5 5-6 6-7 7-8				8	-9	9-10			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8050		
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8051	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/52
Out-of- bounds Read	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8052	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/53
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/54
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	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-2019-8053		
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8054	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/55
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8055	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/56
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/57
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	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-2019-8056		
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8057	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/58
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8058	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/59
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/60
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish D	ate	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
				vul exp	lier have nerabili ploitation pitrary co	ty. Succe n could l	essful ead to	е				
				CV	E ID : CV	/E-2019	-8059					
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	20-08-20	019	10	ver ear ear ear ear ear vul exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8060					https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html		
				CV	E ID : CV	/E-2019	-8060					
Use After Free	20-08-2	019	7.5	ver ear ear ear ear ear vul exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8061				https://elpx.ad e.com// urity/p ducts/a obat/aj 19- 41.htm	ob sec oro acr psb	A-A ACR 060	_
Out-of- bounds Read	20-08-20	019	5	ver ear ear ear ear	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and					/h ob sec oro acr psb	A-A ACF 060	
CV Scoring Scale (CVSS)	0-1	1-2	2	2-3	3-4	4-5	5-6	6-7	6-7 7-8		-9	9-10

Weakness	Publish Da	te	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
				rea exp	d vulner loitatio							
				CVI	E ID : CV	E-2019	-8077					
Out-of- bounds Read	20-08-202	19 !	5	ver ear ear ear ear ear ear info	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8094					/h ob sec ro acr osb	A-ADO- ACRO- 060919/64	
Out-of- bounds Read	20-08-203	19 !	5	ver ear ear ear ear ear rea exp	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8095				https://elpx.ade e.com/s urity/p ducts/a obat/ap 19- 41.htm	ob sec ro ncr osb	A-A ACR 060	
Out-of- bounds Read	20-08-203	19 !	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and					https://elpx.ade.com/surity/pducts/aobat/ap19-41.html	ob sec ro acr osb	A-A ACR 060	
CV Scoring Scale (CVSS)	0-1	1-2	2	-3	3-4	4-5	5-6	6-7	7-8 8-9		-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8096		
Information Exposure	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an internal ip disclosure vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8097	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/67
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8098	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/68
Integer Overflow or Wraparoun d	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/69
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8099		
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8100	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/70
Integer Overflow or Wraparoun d	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8101	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/71
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/72
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8102		
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8103	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/73
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8104	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/74
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/75
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.		
			CVE ID : CVE-2019-8105		
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/76
			CVE ID : CVE-2019-8106		
acrobat_rea	der_dc				
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-7965	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/77
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/78
CV Scoring Scale (CVSS)	e 0-1 1-2	2 2	•	19-	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8002	41.html	
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8003	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/79
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8004	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/80
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/81

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8005	41.html	
NULL Pointer Dereferenc e	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution.	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/82
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8007	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/83
Out-of- bounds Write	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/84

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8008	41.html	
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8009	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/85
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8010	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/86
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/87

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8011	41.html	
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8012	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/88
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8013	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/89
Improper Restriction of Operations within the Bounds of a Memory	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/90

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Buffer			earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8014	41.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8015	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/91
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8016	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/92
NULL Pointer Dereferenc e	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/93

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8017	41.html	
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8018	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/94
Incorrect Type Conversion or Cast	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8019	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/95
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/96

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8020	41.html	
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8021	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/97
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8022	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/98
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/99

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8023	41.html	
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8024	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/100
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8025	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/101
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/102

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8026	41.html	
Out-of- bounds Write	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8027	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/103
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8028	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/104
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/105

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8029	41.html	
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8030	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/106
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8031	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/107
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/108

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8032	41.html	
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8033	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/109
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8034	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/110
Out-of- bounds Read	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/111

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8035	41.html	
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8036	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/112
Out-of- bounds Read	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8037	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/113
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/114

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8038	41.html	
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8039	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/115
Out-of- bounds Read	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8040	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/116
Improper Restriction of Operations within the Bounds of a Memory	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/117

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Buffer			earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8041	41.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8042	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/118
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8043	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/119
Double Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/120

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8044	41.html	
NULL Pointer Dereferenc e	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8045	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/121
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8046	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/122
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/123

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8047	41.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8048	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/124
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	10	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8049	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/125
Improper Restriction of Operations within the Bounds of a Memory	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/126

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			earlier, and 2015.006.30498 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8050	41.html	
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8051	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/127
Out-of- bounds Read	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8052	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/128
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/129

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8053	41.html	
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8054	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/130
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8055	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/131
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/132

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8056	41.html	
Use After Free	20-08-2019	6.8	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8057	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/133
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8058	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/134
Use After Free	20-08-2019	4.3	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/135

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . CVE ID: CVE-2019-8059	41.html	
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	20-08-2019	10	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8060	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/136
Use After Free	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8061	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/137
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/138

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8077	41.html	
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8094	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/139
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8095	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/140
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/141

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8096	41.html	
Information Exposure	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an internal ip disclosure vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8097	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/142
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8098	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/143
Integer Overflow or Wraparoun d	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/144

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8099	41.html	
Out-of- bounds Write	20-08-2019	7.5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8100	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/145
Integer Overflow or Wraparoun d	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8101	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/146
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/147

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8102	41.html	
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8103	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/148
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. CVE ID: CVE-2019-8104	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19- 41.html	A-ADO- ACRO- 060919/149
Out-of- bounds Read	20-08-2019	5	Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and	https://h elpx.adob e.com/sec urity/pro ducts/acr obat/apsb 19-	A-ADO- ACRO- 060919/150

Weakness	Publish Date	cvss		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
			ear rea exp info	lier have d vulner oloitation ormation	2015.00 e an out- rability. S n could l n disclos VE-2019	of-boun Successfead to eure.	ıds	41.htm	l		
Out-of- bounds Read	20-08-2019	5	ver ear ear ear ear ear ear rea exp	rsions, 20 lier, 201 lier, 201 lier, 201 lier, 201 lier, and lier have d vulner ormation	obat and 019.012.2 9.012.2 7.011.3 7.011.3 5.006.3 2015.0 e an out- rability. 3 n could l n disclos	.20035 an 0035 an 0142 an 0143 an 0497 an 06.3049 of-boun Successife ead to	d d d d d 8 and	https://elpx.ad e.com/s urity/p ducts/a obat/ap 19- 41.htm	ob sec ro acr osb	A-A: ACR 060	_
creative_clo	ud										
N/A	16-08-2019	5	Apy ear vul exp of s	Creative Cloud Desktop Application versions 4.6.1 and earlier have a security bypass vulnerability. Successful exploitation could lead to denial of service. CVE ID: CVE-2019-7957				https://elpx.ad e.com/s urity/p ducts/d ative- cloud/a b19- 39.htm	ob sec ro cre	A-A CRE 060	
N/A	16-08-2019	10	Apy ear per Suc to p	Creative Cloud Desktop Application versions 4.6.1 and earlier have an insecure inherited permissions vulnerability. Successful exploitation could lead to privilege escalation. CVE ID: CVE-2019-7958				https://h elpx.adob e.com/sec urity/pro ducts/cre ative- cloud/aps b19- 39.html		A-A CRE 060	
Improper	16-08-2019	10	Creative Cloud Desktop					https://h		A-A	DO-
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	Des	Description & CVE ID					N	CIIPC ID
Input Validation			earlier hav with know vulnerabili exploitation arbitrary co	Application versions 4.6.1 and earlier have a using components with known vulnerabilities vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7959						A- 919/154
Information Exposure	16-08-2019	5	Creative Cl Application versions hat transmission vulnerabilities exploitation information CVE ID : CV	n 4.6.1 an ave an in on of sen ty. Succe n could l n leakag	nd earlie secure sitive da essful ead to e.		https://elpx.ade.com/surity/pducts/cative-cloud/ab19-39.htm	ob sec ero ere	A-A CRE 060	_
photoshop_c	cc									
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	26-08-2019	10	19.1.8 and earlier hav vulnerabili exploitation arbitrary co	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7968				/h ob sec oro oho /a	A-A PHC 060	
Incorrect Type Conversion or Cast	26-08-2019	10	19.1.8 and earlier and 20.0.5 and earlier have a type confusion vulnerability. Successful elpx.adob e.com/sec urity/pro		e.com/sec urity/pro ducts/pho toshop/a psb19-		A-A PHO 060			
Incorrect Type Conversion or Cast	26-08-2019	10	Adobe Pho 19.1.8 and earlier hav vulnerabili exploitatio	https:// elpx.ade e.com/s urity/p ducts/p	ob sec ro	A-A PHC 060				
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	3-4 4-5 5-6 6-7				8-	-9	9-10

Weakness	Publish Date	cvss	Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
			arbitrary co				toshop, psb19- 44.html			
Incorrect Type Conversion or Cast	26-08-2019	10	Adobe Pho 19.1.8 and earlier hav vulnerabili exploitation arbitrary co	https://elpx.adde.com/surity/pducts/ptoshop/psb19-44.html	ob sec ro oho /a	A-A PHO 060				
Incorrect Type Conversion or Cast	26-08-2019	10	Adobe Pho 19.1.8 and earlier hav vulnerabili exploitation arbitrary co	https://elpx.ade e.com/s urity/p ducts/p toshop/ psb19- 44.html	ob sec ro oho /a	A-A PHO 060				
Incorrect Type Conversion or Cast	26-08-2019	10	19.1.8 and earlier hav vulnerabili exploitation arbitrary co	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7973				/h ob sec ro oho /a	A-A PHO 060	
Incorrect Type Conversion or Cast	26-08-2019	10	Adobe Pho 19.1.8 and earlier hav vulnerabili exploitation arbitrary co	5 and	https://elpx.adde.com/surity/pducts/ptoshop/psb19-44.html	ob sec ro oho /a	A-A PHO 060			
Incorrect Type Conversion or Cast	26-08-2019	10	Adobe Pho 19.1.8 and earlier hav vulnerabili exploitatio	5 and	https://h elpx.adob e.com/sec urity/pro ducts/pho		060919/163			
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-	-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			arbitrary code execution. CVE ID: CVE-2019-7975	toshop/a psb19- 44.html		
Out-of- bounds Write	26-08-2019	9.3	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7976	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/164	
Out-of- bounds Read	26-08-2019	4.3	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound read vulnerability. Successful exploitation could lead to memory leak. CVE ID: CVE-2019-7977	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/165	
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7978	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/166	
Out-of- bounds Write	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7979	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/167	
Incorrect Type Conversion or Cast	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a type confusion vulnerability. Successful exploitation could lead to	https://h elpx.adob e.com/sec urity/pro ducts/pho	060919/168	
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			arbitrary code execution. CVE ID: CVE-2019-7980	toshop/a psb19- 44.html		
Out-of- bounds Read	26-08-2019	4.3	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound read vulnerability. Successful exploitation could lead to memory leak. CVE ID: CVE-2019-7981	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/169	
Out-of- bounds Write	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7982	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/170	
Out-of- bounds Write	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7983	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/171	
Out-of- bounds Write	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7984	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/172	
Improper Restriction of Operations within the	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a heap overflow vulnerability. Successful exploitation could lead to	https://h elpx.adob e.com/sec urity/pro ducts/pho	060919/173	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10	

Weakness	Publish Date	cvss	Desc	ription 8	CVE ID		Patch)	N	CIIPC ID
Bounds of a Memory Buffer			arbitrary co				toshop, psb19- 44.html			
Out-of- bounds Write	26-08-2019	6.8	Adobe Phot 19.1.8 and e earlier have write vulne exploitation arbitrary co	https://elpx.adde.com/surity/pducts/ptoshop/psb19-44.html	ob sec ro oho /a	A-A PHC 060				
Out-of- bounds Read	26-08-2019	4.3	Adobe Phot 19.1.8 and e earlier have vulnerabilit exploitation memory lea CVE ID : CV	https://elpx.ade e.com/s urity/p ducts/p toshop/ psb19- 44.html	ob sec ro oho /a	A-A PHC 060				
Out-of- bounds Write	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7988				https://elpx.adde.com/surity/pducts/ptoshop/psb19-44.html	ob sec ro oho /a	A-A PHO 060	
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	26-08-2019	6.8	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7989				N/A		A-A PHO 060	
Improper Restriction of Operations	26-08-2019	10	Adobe Phot 19.1.8 and e earlier have vulnerabilit	5 and	https://h elpx.adob e.com/sec urity/pro		A-ADO- PHOT- 060919/178			
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Patch	1	N	CIIPC ID	
within the Bounds of a Memory Buffer			arb	oloitation oitrary co	ode exec	ution.		ducts/p toshop, psb19- 44.htm	/a		
Out-of- bounds Read	26-08-2019	6.8	19. ear vul exp me	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound read vulnerability. Successful exploitation could lead to memory leak. CVE ID: CVE-2019-7991					/h ob sec oro oho /a	A-A PHC 060	
Out-of- bounds Write	26-08-2019	10	19. ear wri exp arb	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7992					/h ob sec oro oho /a	A-A PHC 060	
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-08-2019	10	19. ear vul exp arb	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7993				https://elpx.ad e.com/s urity/p ducts/p toshop/ psb19- 44.htm	ob sec oro oho /a	A-A PHO 060	
Out-of- bounds Write	26-08-2019	9.3	19. ear wri exp arb	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7994				https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html		A-A PHO 060	
Out-of- bounds Read	26-08-2019	6.8	19. ear	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound read vulnerability. Successful					/h ob sec ro	A-A PHC 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3						8	-9	9-10

Weakness	Publish Date	cvss		Desc	Patch	1	N	CIIPC ID			
			mei	loitatior mory lea	ık.			ducts/p toshop, psb19- 44.htm	/a		
Out-of- bounds Read	26-08-2019	6.8	19.1 earl vuli exp mei	obe Phot 1.8 and of lier have nerabilit loitation mory lea E ID : CV	nd 20.0. of bound ssful ead to	https://elpx.ade.com/surity/pducts/ptoshop/psb19-44.html	ob sec ro oho /a	A-A PHO 060			
Out-of- bounds Write	26-08-2019	10	19.2 earl wri exp arb	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7997					/h ob sec ro oho /a	A-A PHO 060	
Out-of- bounds Write	26-08-2019	10	19.1 earl wri exp arb	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-7998					/h ob sec ro oho /a	A-A PHO 060	
Out-of- bounds Read	26-08-2019	4.3	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound read vulnerability. Successful exploitation could lead to memory leak. CVE ID: CVE-2019-7999					https://elpx.ade e.com/s urity/p ducts/p toshop/ psb19- 44.html	ob sec ro oho /a	A-A PHO 060	
Out-of- bounds Read	26-08-2019	4.3	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound read vulnerability. Successful					https://h elpx.adob e.com/sec urity/pro		A-ADO- PHOT- 060919/188	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	2-3 3-4 4-5 5-6 6-7					7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to memory leak. CVE ID: CVE-2019-8000	ducts/pho toshop/a psb19- 44.html	
Out-of- bounds Write	26-08-2019	10	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have an out of bound write vulnerability. Successful exploitation could lead to arbitrary code execution. CVE ID: CVE-2019-8001	https://h elpx.adob e.com/sec urity/pro ducts/pho toshop/a psb19- 44.html	A-ADO- PHOT- 060919/189
experience_	manager				
Improper Authenticat ion	16-08-2019	10	Adobe Experience Manager versions 6.5, and 6.4 have an authentication bypass vulnerability. Successful exploitation could lead to remote code execution. CVE ID: CVE-2019-7964	https://h elpx.adob e.com/sec urity/pro ducts/exp erience- manager/ apsb19- 42.html	A-ADO- EXPE- 060919/190
adplug_proj	ect			<u>'</u>	
adplug					
Double Free	18-08-2019	7.5	AdPlug 2.3.1 has a double free in the Cu6mPlayer class in u6m.h. CVE ID: CVE-2019-15151	N/A	A-ADP- ADPL- 060919/191
Alfresco					
alfresco					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL	26-08-2019	7.5	The Alfresco application before 1.8.7 for Android allows SQL injection in HistorySearchProvider.java. CVE ID: CVE-2019-15566	N/A	A-ALF-ALFR- 060919/192
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-					

ish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
emplate				
8-2019	4.3	In the Alkacon OpenCms Apollo Template 10.5.4 and 10.5.5, there is XSS in the search engine. CVE ID: CVE-2019-13234	N/A	A-ALK- OPEN- 060919/193
8-2019	4.3	In the Alkacon OpenCms Apollo Template 10.5.4 and 10.5.5, there is XSS in the Login form. CVE ID: CVE-2019-13235	N/A	A-ALK- OPEN- 060919/194
8-2019	4	In Alkacon OpenCms 10.5.4 and 10.5.5, there are multiple resources vulnerable to Local File Inclusion that allow an attacker to access server resources: clearhistory.jsp, convertxml.jsp, group_new.jsp, loginmessage.jsp, xmlcontentrepair.jsp, and /system/workplace/admin/history/settings/index.jsp. CVE ID: CVE-2019-13237	N/A	A-ALK- OPEN- 060919/195
8-2019	4.3	In system/workplace/ in Alkacon OpenCms 10.5.4 and 10.5.5, there are multiple Reflected and Stored XSS issues in the management interface. CVE ID: CVE-2019-13236	N/A	A-ALK- OPEN- 060919/196
8-20	019	019 4.3	are multiple Reflected and Stored XSS issues in the management	are multiple Reflected and Stored XSS issues in the management interface.

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
altavoz					
prontuscms					
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	26-08-2019	10	cgi- cpn/xcoding/prontus_videocut.cg i in AltaVoz Prontus (aka ProntusCMS) through 12.0.3.0 has "Improper Neutralization of Special Elements used in an OS Command," allowing attackers to execute OS commands via an HTTP GET parameter. CVE ID: CVE-2019-15503	N/A	A-ALT- PRON- 060919/197
Ampache					
ampache					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	22-08-2019	6.5	An issue was discovered in Ampache through 3.9.1. The search engine is affected by a SQL Injection, so any user able to perform lib/class/search.class.php searches (even guest users) can dump any data contained in the database (sessions, hashed passwords, etc.). This may lead to a full compromise of admin accounts, when combined with the weak password generator algorithm used in the lostpassword functionality. CVE ID: CVE-2019-12385	N/A	A-AMP- AMPA- 060919/198
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	22-08-2019	3.5	An issue was discovered in Ampache through 3.9.1. A stored XSS exists in the localplay.php LocalPlay "add instance" functionality. The injected code is reflected in the instances menu. This vulnerability can be abused	N/A	A-AMP- AMPA- 060919/199
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	NC	IIPC ID
Scripting')			to force an admin to create a new privileged user whose credentials are known by the attacker.			
			CVE ID : CVE-2019-12386			
Apache						
commons_be	eanutils					
Deserializat ion of Untrusted Data	20-08-2019	7.5	In Apache Commons Beanutils 1.9.2, a special BeanIntrospector class was added which allows suppressing the ability for an attacker to access the classloader via the class property available on all Java objects. We, however were not using this by default characteristic of the PropertyUtilsBean. CVE ID: CVE-2019-10086	N/A	A-AP. COMI 0609	
Artica			CVE ID : CVE-2017-10000			
integria_ims						
Unrestricte d Upload of File with Dangerous Type	16-08-2019	7.5	filemgr.php in Artica Integria IMS 5.0.86 allows index.php?sec=wiki&sec2=operation/wiki/wiki&action=upload arbitrary file upload. CVE ID: CVE-2019-15091	N/A		T-INTE- 19/201
aspose						
aspose.cells						
Out-of- bounds Read	21-08-2019	6.8	An exploitable out-of-bounds read vulnerability exists in the LabelSst record parser of Aspose Aspose.Cells 19.1.0 library. A specially crafted XLS file can cause an out-of-bounds read, resulting in remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	N/A		P-ASPO- 19/202
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 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-2019-5032		
Out-of- bounds Read	21-08-2019	6.8	An exploitable out-of-bounds read vulnerability exists in the Number record parser of Aspose Aspose. Cells 19.1.0 library. A specially crafted XLS file can cause an out-of-bounds read, resulting in remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability. CVE ID: CVE-2019-5033	N/A	A-ASP-ASPO- 060919/203
aspose.word	ls				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-08-2019	6.8	An exploitable Stack Based Buffer Overflow vulnerability exists in the EnumMetaInfo function of Aspose Aspose.Words library, version 18.11.0.0. A specially crafted doc file can cause a stack-based buffer overflow, resulting in remote code execution. An attacker needs to provide a malformed file to the victim to trigger this vulnerability. CVE ID: CVE-2019-5041	N/A	A-ASP-ASPO- 060919/204
assign-deep	_project				
assign-deep					
Improper Input Validation	20-08-2019	5	assign-deep is vulnerable to Prototype Pollution in versions before 0.4.8 and version 1.0.0. The function assign-deep could be tricked into adding or modifying properties of Object.prototype using either a constructor or a _proto_ payload. CVE ID : CVE-2019-10745	https://sn yk.io/vuln /SNYK-JS- ASSIGND EEP- 450211	A-ASS-ASSI- 060919/205
Atlassian					

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

Weakness	Publish Date	cvss	Description & CVE ID	Patch	N	ICIIPC ID
jira						
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	The MigratePriorityScheme resource in Jira before version 8.3.2 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the priority icon url of an issue priority. CVE ID: CVE-2019-11584	N/A		TL-JIRA- 1919/206
URL Redirection to Untrusted Site ('Open Redirect')	23-08-2019	5.8	The startup.jsp resource in Jira before version 7.13.6, from version 8.0.0 before version 8.2.3, and from version 8.3.0 before version 8.3.2 allows remote attackers to redirect users to a different website which they may use as part of performing a phishing attack via an open redirect. CVE ID: CVE-2019-11585	N/A	I	TL-JIRA- 1919/207
Cross-Site Request Forgery (CSRF)	23-08-2019	4.3	The AddResolution.jspa resource in Jira before version 7.13.6, from version 8.0.0 before version 8.2.3, and from version 8.3.0 before version 8.3.2 allows remote attackers to create new resolutions via a Cross-site request forgery (CSRF) vulnerability. CVE ID: CVE-2019-11586	N/A		TL-JIRA- 1919/208
Cross-Site Request Forgery (CSRF)	23-08-2019	4.3	Various exposed resources of the ViewLogging class in Jira before version 7.13.6, from version 8.0.0 before version 8.2.3, and from version 8.3.0 before version 8.3.2 allow remote attackers to modify various settings via Cross-site request forgery (CSRF).	N/A		TL-JIRA- 919/209
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 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-2019-11587		
Cross-Site Request Forgery (CSRF)	23-08-2019	4.3	The ViewSystemInfo class doGarbageCollection method in Jira before version 7.13.6, from version 8.0.0 before version 8.2.3, and from version 8.3.0 before version 8.3.2 allows remote attackers to trigger garbage collection via a Cross-site request forgery (CSRF) vulnerability. CVE ID: CVE-2019-11588	N/A	A-ATL-JIRA- 060919/210
URL Redirection to Untrusted Site ('Open Redirect')	23-08-2019	5.8	The ChangeSharedFilterOwner resource in Jira before version 7.13.6, from version 8.0.0 before version 8.2.3, and from version 8.3.0 before version 8.3.2 allows remote attackers to attack users, in some cases be able to obtain a user's Cross-site request forgery (CSRF) token, via a open redirect vulnerability. CVE ID: CVE-2019-11589	N/A	A-ATL-JIRA- 060919/211
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	3.5	The wikirenderer component in Jira before version 7.13.6, and from version 8.0.0 before version 8.3.2 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in image attribute specification. CVE ID: CVE-2019-8444	N/A	A-ATL-JIRA- 060919/212
N/A	23-08-2019	5	Several worklog rest resources in Jira before version 7.13.7, and from version 8.0.0 before version 8.3.2 allow remote attackers to view worklog time information via a missing permissions check. CVE ID: CVE-2019-8445	N/A	A-ATL-JIRA- 060919/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authorizati on	23-08-2019	5	The /rest/issueNav/1/issueTable resource in Jira before version 8.3.2 allows remote attackers to enumerate usernames via an incorrect authorisation check. CVE ID: CVE-2019-8446	N/A	A-ATL-JIRA- 060919/214
Cross-Site Request Forgery (CSRF)	23-08-2019	4.3	The ServiceExecutor resource in Jira before version 8.3.2 allows remote attackers to trigger the creation of export files via a Cross-site request forgery (CSRF) vulnerability. CVE ID: CVE-2019-8447	N/A	A-ATL-JIRA- 060919/215
universal_pl	ugin_manage	r			
Cross-Site Request Forgery (CSRF)	23-08-2019	4.3	The Uninstall REST endpoint in Atlassian Universal Plugin Manager before version 2.22.19, from version 3.0.0 before version 3.0.3 and from version 4.0.0 before version 4.0.3 allows remote attackers to uninstall plugins using a Cross-Site Request Forgery (CSRF) vulnerability on an authenticated administrator. CVE ID: CVE-2019-14999	N/A	A-ATL-UNIV 060919/216
Audiocoding	3				
freeware_ad	lvanced_audio	o_deco	der_2		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-08-2019	6.8	An issue was discovered in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The faad_resetbits function in libfaad/bits.c is affected by a buffer overflow vulnerability. The number of bits to be read is determined by ld->buffer_size - words*4, cast to uint32. If ld- >buffer_size - words*4 is	N/A	A-AUD- FREE- 060919/217

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			negative, a buffer overflow is later performed via getdword_n(&ld->start[words], ld->bytes_left). CVE ID: CVE-2019-15296						
Autodesk									
design_revie	ew								
Untrusted Search Path	23-08-2019	6.8	DLL preloading vulnerability in Autodesk Design Review versions 2011, 2012, 2013, and 2018. An attacker may trick a user into opening a malicious DWF file that may leverage a DLL preloading vulnerability, which may result in code execution. CVE ID: CVE-2019-7362	https://w ww.autod esk.com/t rust/secu rity- advisories /adsk-sa- 2019- 0002	A-AUT-DESI- 060919/218				
Use After Free	23-08-2019	6.8	Use-after-free vulnerability in Autodesk Design Review versions 2011, 2012, 2013, and 2018. An attacker may trick a user into opening a malicious DWF file that may leverage a use-after-free vulnerability, which may result in code execution. CVE ID: CVE-2019-7363	https://w ww.autod esk.com/t rust/secu rity- advisories /adsk-sa- 2019- 0002	A-AUT-DESI- 060919/219				
Bedita									
bedita									
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	26-08-2019	7.5	BEdita through 4.0.0-RC2 allows SQL injection during a save operation for a relation with parameters. CVE ID: CVE-2019-15570	N/A	A-BED-BEDI- 060919/220				

6-7

7-8

8-9

9-10

2-3

3-4

4-5

1-2

0-1

CV Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
belwith-kee	ler				
hickory_sma	nrt				
Information Exposure	22-08-2019	2.1	An insecure storage of sensitive information vulnerability is present in Hickory Smart for Android mobile devices from Belwith Products, LLC. The application's database was found to contain information that could be used to control the lock devices remotely. This issue affects Hickory Smart for Android, version 01.01.43 and prior versions. CVE ID: CVE-2019-5632	N/A	A-BEL-HICK- 060919/221
Information Exposure	22-08-2019	2.1	An insecure storage of sensitive information vulnerability is present in Hickory Smart for iOS mobile devices from Belwith Products, LLC. The application's database was found to contain information that could be used to control the lock devices remotely. This issue affects Hickory Smart for iOS, version 01.01.07 and prior versions. CVE ID: CVE-2019-5633	N/A	A-BEL-HICK- 060919/222
Information Exposure Through Log Files	22-08-2019	2.1	An inclusion of sensitive information in log files vulnerability is present in Hickory Smart for Android mobile devices from Belwith Products, LLC. Communications to the internet API services and direct connections to the lock via Bluetooth Low Energy (BLE) from the mobile application are logged in a debug log on the Android device at	N/A	A-BEL-HICK- 060919/223

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVS	5	Des	cription 8	& CVE ID		Patch	1	NCIIPC ID
			fou dev sto wit iss An pri	Log.txt. This information was found stored in the Android device's default USB or SDcard storage paths and is accessible without rooting the device. This issue affects Hickory Smart for Android, version 01.01.43 and prior versions. CVE ID: CVE-2019-5634						
bloodhound	_project									
bloodhound										
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	27-08-2019	6.8	sx rer arb spa cui ma fur is u dat with in it	components/Modals/HelpModal.j sx in BloodHound 2.2.0 allows remote attackers to execute arbitrary OS commands (by spawning a child process as the current user on the victim's machine) when the search function's autocomplete feature is used. The victim must import data from an Active Directory with a GPO containing JavaScript in its name. CVE ID: CVE-2019-15701		N/A	E	A-BLO- BLOO- 060919/224		
Bolt										
bolt										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	titl sys	Bolt before 3.6.10 has XSS via a title that is mishandled in the system log. CVE ID: CVE-2019-15483			N/A	E	A-BOL- BOLT- 060919/225	
Improper Neutralizati on of Input	23-08-2019	4.3	im	Bolt before 3.6.10 has XSS via an image's alt or title field. CVE ID: CVE-2019-15484					E	A-BOL- BOLT- B60919/226
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
During Web Page Generation ('Cross-site Scripting')					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	Bolt before 3.6.10 has XSS via createFolder or createFile in Controller/Async/FilesystemMan ager.php. CVE ID: CVE-2019-15485	N/A	A-BOL- BOLT- 060919/227
cdemu					
libmirage					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-08-2019	7.2	filters/filter-cso/filter-stream.c in the CSO filter in libMirage 3.2.2 in CDemu does not validate the part size, triggering a heap-based buffer overflow that can lead to root access by a local Linux user. CVE ID: CVE-2019-15540	N/A	A-CDE-LIBM- 060919/228
centos-webj	oanel				
centos_web_	panel				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-08-2019	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.837, XSS in the domain parameter allows a low-privilege user to achieve root access via the email list page. CVE ID: CVE-2019-13476		N/A	A-CEN- CENT- 060919/229
Cross-Site Request Forgery (CSRF)	21-08-2019	4.3	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.837, CSRF in the forgot password function allows an attacker to change the password	N/A	A-CEN- CENT- 060919/230

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	N	ICIIPC ID
			for the root account.			
			CVE ID: CVE-2019-13477			
Information Exposure	21-08-2019	5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.848, the Login process allows attackers to check whether a username is valid by comparing response times. CVE ID: CVE-2019-13599	N/A	CEN	EN- NT- 1919/231
N/A	21-08-2019	5.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to delete databases (such as oauthv2) from the server via an attacker account. CVE ID: CVE-2019-14245	N/A	CEN	EN- NT- 0919/232
N/A	21-08-2019	4	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to discover phpMyAdmin passwords (of any user in /etc/passwd) via an attacker account.	N/A	CEN	EN- NT- 0919/233
			CVE ID : CVE-2019-14246			
Cisco						
unified_cont	act_center_ex	press			Ţ	
Improper Input Validation	21-08-2019	3.5	A vulnerability in the web-based management interface of Cisco Unified Contact Center Express (Unified CCX) 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 vulnerability	N/A		IS-UNIF- 1919/234
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Desc	cription 8	CVE ID		Patcl	h	N	CIIPC ID
			is due to insufficient validation of user-supplied input by the webbased management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker needs valid administrator credentials. CVE ID: CVE-2019-12626							
ucs_director										
Use of Hard-coded Credentials	21-08-2019	10	A vulnerability in Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to log in to the CLI of an affected system by using the SCP User account (scpuser), which has default user credentials. The vulnerability is due to the presence of a documented default account with an undocumented default password and incorrect permission settings for that account. Changing the default password for this account is not enforced during the installation of the product. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful				N/A		A-CIS-UCS 060919/235	
CV Scoring Scale (CVSS)	0-1 1-7	2 2	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 Input Validation	21-08-2019	9	exploit could allow the attacker to execute arbitrary commands with the privileges of the scpuser account. This includes full read and write access to the system's database. CVE ID: CVE-2019-1935 A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an authenticated, remote attacker to execute arbitrary commands on the underlying Linux shell as the root user. Exploitation of this vulnerability requires privileged access to an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by logging in to the web-based management interface with administrator privileges and then sending a malicious request to a certain part of the interface. CVE ID: CVE-2019-1936	N/A	A-CIS-UCS 060919/236
Improper Authenticat ion	21-08-2019	10	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to acquire a valid session token with administrator	N/A	A-CIS-UCS 060919/237
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7 73	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges, bypassing user authentication. The vulnerability is due to insufficient request header validation during the authentication process. An attacker could exploit this vulnerability by sending a series of malicious requests to an affected device. An exploit could allow the attacker to use the acquired session token to gain full administrator access to the affected device. CVE ID: CVE-2019-1937		
Improper Authenticat ion	21-08-2019	10	A vulnerability in the web-based management interface of Cisco UCS Director and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrator privileges on an affected system. The vulnerability is due to improper authentication request handling. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow an unprivileged attacker to access and execute arbitrary actions through certain APIs. CVE ID: CVE-2019-1938	N/A	A-CIS-UCS 060919/238
Improper Authenticat ion	21-08-2019	10	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data	N/A	A-CIS-UCS 060919/239
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7 74	7-8	8-9 9-10

Weakness	Publish Dat	te C	VSS		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
				ren aut an a vul req the atta vul of r affe adr affe	henticat henticat adminis nerabili- quest hea authent acker co- nerabili- maliciou ected de- ow the at ministrate		bypass ugain access. Oit this action access. It to an exploit access to the exploit acce	ficient luring An eries could				
N/A	21-08-201	19 5		A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to a missing authentication check in an API call. An attacker who can send a request to an affected system could cause all currently authenticated users to be logged off. Repeated exploitation could cause the inability to maintain a session in the web-based management portal. CVE ID: CVE-2019-12634				N/A			IS-UCS 919/240	
ucs_director	_express_f	or_bi	g_da	ta								
Use of Hard-coded Credentials	21-08-201	19 1	0	A vulnerability in Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS					N/A		A-CIS-UCS 060919/241	
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	Desc	cription 8	CVE ID		Patch	1	N	CIIPC ID
			Director Ex could allow remote atta CLI of an aff the SCP Use which has done to the produce an undocumpassword a permission account. Che password for the produce and the account affected system of the produce and the account affected system of the produce and the produce and the account affected system of the produce and write and write a database. CVE ID: CV	an unaucker to be fected system account of the vulle or esence of default in the fect of t	ithentic log in to vistem by at (scpu ser nerability of a taccount in the default execunt in tacker bility by a to an uccessful the attact of the scound of the scound in the system of	ated, the vusing ser), tty is at with t ult s not ation could vusing ul cker ands cpuser read				
Improper Input Validation	21-08-2019	9	A vulnerabi managemen Integrated I Controller (Cisco UCS Director Excould allow remote attarbitrary counderlying user. Exploivulnerabilit access to an vulnerabilit validation of	Manager (IMC) Surfector, press for an authorized command Linux shall tation on affected by is due	ace of Cinent pervisor and Cisor Big Da enticate execute s on the hell as the f this res privi d device to insuf	r, co UCS ta ed, he root leged . The	N/A			IS-UCS 919/242
CV Scoring Scale (CVSS)	0-1 1-2	2 2	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by the web-based management interface. An attacker could exploit this vulnerability by logging in to the web-based management interface with administrator privileges and then sending a malicious request to a certain part of the interface. CVE ID: CVE-2019-1936		
Improper Authenticat ion	21-08-2019	10	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to acquire a valid session token with administrator privileges, bypassing user authentication. The vulnerability is due to insufficient request header validation during the authentication process. An attacker could exploit this vulnerability by sending a series of malicious requests to an affected device. An exploit could allow the attacker to use the acquired session token to gain full administrator access to the affected device. CVE ID: CVE-2019-1937	N/A	A-CIS-UCS 060919/243
Improper Authenticat ion	21-08-2019	10	A vulnerability in the web-based management interface of Cisco UCS Director and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with	N/A	A-CIS-UCS 060919/244
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7 77	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			administrator privileges on an affected system. The vulnerability is due to improper authentication request handling. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow an unprivileged attacker to access and execute arbitrary actions through certain APIs. CVE ID: CVE-2019-1938		
Improper Authenticat ion	21-08-2019	10	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to bypass user authentication and gain access as an administrative user. The vulnerability is due to insufficient request header validation during the authentication process. An attacker could exploit this vulnerability by sending a series of malicious requests to an affected device. An exploit could allow the attacker to gain full administrative access to the affected device. CVE ID: CVE-2019-1974	N/A	A-CIS-UCS 060919/245
N/A	21-08-2019	5	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated,	N/A	A-CIS-UCS 060919/246
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	9 (cvss		Des	cription 8	& CVE ID		Patch)	N	CIIPC ID
				remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to a missing authentication check in an API call. An attacker who can send a request to an affected system could cause all currently authenticated users to be logged off. Repeated exploitation could cause the inability to maintain a session in the web-based management portal. CVE ID: CVE-2019-12634								
unified_com	puting_syst	em										
Improper Input Validation	21-08-201	99 3		A vulnerability in the Intelligent Platform Management Interface (IPMI) of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges on the underlying operating system (OS). The vulnerability is due to insufficient input validation of user-supplied commands. An attacker who has administrator privileges and access to the network where the IPMI resides could exploit this vulnerability by submitting crafted input to the affected commands. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID: CVE-2019-1634				N/A			IS-UNIF- 919/247	
Improper Authorizati on	21-08-201	9 6	6.5	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to					N/A			IS-UNIF- 919/248
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
			set sensitive configuration values and gain elevated privileges. The vulnerability is due to improper handling of substring comparison operations that are performed by the affected software. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow the attacker with read-only privileges to gain administrator privileges.		
			CVE ID: CVE-2019-1907		
Information Exposure	21-08-2019	5	A vulnerability in the Intelligent Platform Management Interface (IPMI) implementation of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to view sensitive system information. The vulnerability is due to insufficient security restrictions imposed by the affected software. A successful exploit could allow the attacker to view sensitive information that belongs to other users. The attacker could then use this information to conduct additional attacks. CVE ID: CVE-2019-1908	N/A	A-CIS-UNIF- 060919/249
Improper Neutralizati on of Special Elements used in an OS Command ('OS	21-08-2019	9	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges on an affected device. An attacker would need to	N/A	A-CIS-UNIF- 060919/250
	0-1 1-	2 2		7-8	8-9 9-1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIPC ID
Command Injection')			have valid administrator credentials on the device. The vulnerability is due to insufficient validation of user-supplied input by the affected software. An attacker with elevated privileges could exploit this vulnerability by sending crafted commands to the administrative web management interface of the affected software. A successful exploit could allow the attacker to inject and execute arbitrary, system-level commands with root privileges on an affected device.			
			CVE ID : CVE-2019-1850			
Improper Authorizati on	21-08-2019	9	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to make unauthorized changes to the system configuration. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow a user with read-only privileges to change critical system configurations using administrator privileges. CVE ID: CVE-2019-1863	N/A		-CIS-UNIF- 60919/251
Improper Neutralizati on of Special Elements	21-08-2019	9	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote	N/A		-CIS-UNIF- 60919/252
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attacker to inject arbitrary commands that are executed with root privileges on an affected device. The vulnerability is due to insufficient validation of command input by the affected software. An attacker could exploit this vulnerability by sending malicious commands to the web-based management interface of the affected software. A successful exploit could allow the attacker, with read-only privileges, to inject and execute arbitrary, system-level commands with root privileges on an affected device.		
			CVE ID : CVE-2019-1864		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	21-08-2019	9	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges on an affected device. The vulnerability is due to insufficient validation of usersupplied input by the affected software. An attacker could exploit this vulnerability by invoking an interface monitoring mechanism with a crafted argument on the affected software. A successful exploit could allow the attacker to inject and execute arbitrary, systemlevel commands with root privileges on an affected device. CVE ID: CVE-2019-1865	N/A	A-CIS-UNIF- 060919/253
CV Scoring Scale	0-1 1-2) 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	N	ICIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-08-2019	9	A vulnerability in the Import Cisco IMC configuration utility of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition and implement arbitrary commands with root privileges on an affected device. The vulnerability is due to improper bounds checking by the import-config process. An attacker could exploit this vulnerability by sending malicious packets to an affected device. When the packets are processed, an exploitable buffer overflow condition may occur. A successful exploit could allow the attacker to implement arbitrary code on the affected device with elevated privileges. CVE ID: CVE-2019-1871	N/A		IS-UNIF- 1919/254
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	21-08-2019	7.2	A vulnerability in the command- line interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker with read-only credentials to inject arbitrary commands that could allow them to obtain root privileges. The vulnerability is due to insufficient validation of user-supplied input on the command-line interface. An attacker could exploit this vulnerability by authenticating with read-only privileges via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow an attacker to	N/A		IS-UNIF- 1919/255
CV Scoring Scale (CVSS)	0-1 1-3	2 2	- 3 3-4 4-5 5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on the device with root privileges. CVE ID: CVE-2019-1883		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	21-08-2019	9	A vulnerability in the Redfish protocol of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to inject and execute arbitrary commands with root privileges on an affected device. The vulnerability is due to insufficient validation of usersupplied input by the affected software. An attacker could exploit this vulnerability by sending crafted authenticated commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to inject and execute arbitrary commands on an affected device with root privileges. CVE ID: CVE-2019-1885	N/A	A-CIS-UNIF- 060919/256
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	21-08-2019	9	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to inject arbitrary commands and obtain root privileges. The vulnerability is due to insufficient validation of user-supplied input in the Certificate Signing Request (CSR) function of the web-based management interface. An attacker could exploit this vulnerability by submitting a crafted CSR in the web-based management interface. A	N/A	A-CIS-UNIF- 060919/257
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Des	Patch		N	CIIPC ID			
			successful attacker w privileges t commands root privile CVE ID : CV A vulnerab of Cisco Int Controller	ith admin to execut on the d eges. VE-2019 ility in the	nistrator te arbitra levice w -1896 ne web s Manage	ary ith full erver ment				
NULL Pointer Dereferenc e	21-08-2019	7.8	unauthenti to cause th to crash, ca service (Do affected sy is due to in user-suppl interface. A exploit this submitting request to the affected successful attacker to to crash. Pl device may restart. CVE ID: CV	emote at rver prodenial of tion on e vulner t validate ton the er could bility by d HTTP indpoint re. A ould allowe web secess to ired for	N/A			S-UNIF- 919/258		
firepower_tl	reat_defense	:								
Improper Access Control	21-08-2019	5	A vulnerable policy configure for Firepower Software connauthentito gain unato sensitive vulnerabilitapplication attacker convulnerabilitraffic to an	iguration Threat E ould allo icated, re outhorize e data. Th ty is due outhorific ould exploity by ser	n of the Oefense (w an emote at ed read a ne to insuffication. A oit this ading cra	N/A			S-FIRE- 919/259	
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	5-6	7-8	8-	9	9-10		

Weakness	Publish Date	cvss	Des	cription 8	Patch		NCIIPC ID		
			successful of attacker to read access	gain una to sensi	uthoriz tive dat	ed			
integrated_r	nanagement_	contro	ller_superv	isor					
Improper Authorizati on	21-08-2019	6.5	A vulnerable of Cisco Interpretation Controller (authenticate set sensitive and gain elevalnerability handling of operations the affected could explose sending a could explose to the affect successful eattacker with the gain admitted CVE ID: CVE	egrated (IMC) co ted, remove configue vated p ty is due that are alsoftware that software ted software that control ted ted software that are ted software that are alsoftware that are alsoftware that are alsoftware that read-ninistrate	Manage uld allow ote attacturation willeges to improperform re. An attached allow only privil	N/A		A-CIS-INTE- 060919/260	
Use of Hard-coded Credentials	21-08-2019	10	A vulnerabilintegrated Controller (Cisco UCS I) Director Excould allowed an afthe SCP Used which has decredentials due to the password apermission account. Chapassword for the password of th	Manager (IMC) Sur- Director, spress for an unauticker to be fected system account default undersence default	ment perviso and Ciso r Big Da Ithentic log in to vstem by nt (scpu ser nerabili of a t accoun lefault rect for that	N/A		A-CIS-INTE- 060919/261	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch	1	N	ICIIPC ID
			enforced du of the prod exploit this the account affected sys exploit cou to execute a with the pr account. Th and write a database. CVE ID: CV	uct. An a vulnera to log in stem. A s ld allow arbitrary ivileges iis includ ccess to	ttacker bility by to an uccessfo the atta comma of the so les full r the syst					
Improper Input Validation	21-08-2019	9	A vulnerable management Integrated Controller Cisco UCS I Director Excould allow remote attain arbitrary counderlying user. Exploit vulnerability access to an vulnerability validation of by the weblinterface. A exploit this logging in the management administration and certain participal in the control of	Manager (IMC) Surficector, an authorization of the weath of the interface of the interface of the weath of the weath of the weath of the interface of the inter	ace of Ciment pervisor and Cisor Big Da enticate execute s on the nell as the f this res privi d device to insuf upplied nanagem er could bility by b-based ace with leges an ereques nterface	r, co UCS ta ed, leged The fficient input nent l	N/A			IS-INTE- 1919/262
Improper Authenticat ion	21-08-2019	10	A vulnerabi manageme Integrated Controller	ace of Ci nent	sco	N/A			IS-INTE- 1919/263	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3 3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to bypass user authentication and gain access as an administrative user. The vulnerability is due to insufficient request header validation during the authentication process. An attacker could exploit this vulnerability by sending a series of malicious requests to an affected device. An exploit could allow the attacker to gain full administrative access to the affected device. CVE ID: CVE-2019-1974		
code42					
code42_for_	enterprise				
N/A	21-08-2019	2.1	In Code42 Enterprise and Crashplan for Small Business through Client version 6.9.1, an attacker can craft a restore request to restore a file through the Code42 app to a location they do not have privileges to write. CVE ID: CVE-2019-11551	https://su pport.cod e42.com/ Terms_an d_conditio ns/Code4 2_custom er_suppor t_resourc es/Code4 2_security _advisorie s/Users_c an_restor e_files_to_ locations_ they_do_n ot_have_w rite_acces s_to	A-COD- CODE- 060919/264

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
crashplan_fo	or_small_busi	ness			
N/A	21-08-2019	2.1	In Code42 Enterprise and Crashplan for Small Business through Client version 6.9.1, an attacker can craft a restore request to restore a file through the Code42 app to a location they do not have privileges to write. CVE ID: CVE-2019-11551	https://su pport.cod e42.com/ Terms_an d_conditio ns/Code4 2_custom er_suppor t_resourc es/Code4 2_security _advisorie s/Users_c an_restor e_files_to_ locations_ they_do_n ot_have_w rite_acces s_to	A-COD- CRAS- 060919/265
Codection		•			
	rs_from_csv_w	rith_me	eta	T	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-08-2019	5	The import-users-from-csv-with-meta plugin before 1.14.2.1 for WordPress has directory traversal. CVE ID: CVE-2019-15326	N/A	A-COD- IMPO- 060919/266
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	22-08-2019	4.3	The import-users-from-csv-with-meta plugin before 1.14.1.3 for WordPress has XSS via imported data. CVE ID: CVE-2019-15327	N/A	A-COD- IMPO- 060919/267

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Improper Neutralization of Input During Web Page Generation ('Cross-Site Request Forgery (CSRF) 22-08-2019 6.8 The import-users-from-csv-with-meta plugin before 1.14.0.3 for WordPress has XSS. CVE ID : CVE-2019-15328 CVE ID : CVE-2019-15328 N/A A-COD-IMPO-060919/268 A-COD-IMPO-060919/268 A-COD-IMPO-060919/269 A-COD-IMP	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting') Cross-Site Request Forgery (CSRF) CVE ID: CVE-2019-15328 The import-users-from-csv-with-meta plugin before 1.14.0.3 for WordPress has XSS. CVE ID: CVE-2019-15328 The import-users-from-csv-with-meta plugin before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-15329 N/A A-COD-IMPO-060919/268 A-COD-IMPO-060919/268 The import-users-from-csv-with-meta plugin before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-15329 N/A A-COD-IMPO-060919/269 Comelz quark Improper Limitation of a Pathname to a P	Scripting')					
Request Forgery (CSRF) Request WordPress has CSRF. CVE ID: CVE-2019-15329 Repose Substitution of a Pathname to a Restricted Directory (Path Traversal') Restricted Directory (Path Traversal') Remain Special Elements used in an SQL Command Request MordPress has CSRF. CVE ID: CVE-2019-15329 Repose Substitution before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-15329 Repose Substitution before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-03-26 Repose Substitution before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-03-29 Repose Substitution before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-15520 Repose Substitution before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-15520 Repose Substitution before 1.14.0.3 for WordPress has CSRF. CVE ID: CVE-2019-15520 Repose Substitution before 1.14.0.3 for N/A A-COM-QUAR-O60919/270 A-COM-COMP-O60919/271 COMP-O60919/271	Neutralizati on of Input During Web Page Generation ('Cross-site	22-08-2019	4.3	meta plugin before 1.14.0.3 for WordPress has XSS.	N/A	
Improper Limitation of a Pathname to a Pathn	Request Forgery	22-08-2019	6.8	meta plugin before 1.14.0.3 for WordPress has CSRF.	N/A	IMPO-
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Compassionus Compassionus The Compassion Switzerland Special Elements used in an SQL Command To a Pathname 23-08-2019 The Compassion Switzerland SQL Command To CVE ID: CVE-2019-15564 Compassion.p. CVE ID: CVE-2019-15564 A-COM- N/A A-COM- N/A A-COM- COMP- 060919/271	comelz					
Limitation of a Pathname to a	quark					
Improper Neutralizati on of Special Elements used in an SQL Command Ze-08-2019 Ze-08-201	Limitation of a Pathname to a Restricted Directory ('Path Traversal')		5	allows directory traversal to locations outside of the project directory.	N/A	QUAR-
Improper Neutralizati on of Special Elements used in an SQL Command The Compassion Switzerland addons 10.01.4 for Odoo allow SQL injection in models/partner_compassion.py. CVE ID: CVE-2019-15564 A-COM- COMP- 060919/271	compassion	uk 				
Neutralizati on of Special Elements used in an SQL Command Neutralizati The Compassion Switzerland addons 10.01.4 for Odoo allow SQL injection in models/partner_compassion.py. CVE ID: CVE-2019-15564 The Compassion Switzerland addons 10.01.4 for Odoo allow SQL injection in models/partner_compassion.py.	-	_switzerland				
Injection')	Neutralizati on of Special Elements used in an SQL Command ('SQL	26-08-2019	7.5	addons 10.01.4 for Odoo allow SQL injection in models/partner_compassion.py.	N/A	COMP-
cszcms	cszcms					<u> </u>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
csz_cms					
Unrestricte d Upload of File with Dangerous Type	26-08-2019	7.5	CSZ CMS 1.2.3 allows arbitrary file upload, as demonstrated by a .php file to admin/filemanager in the File Management Module, which leads to remote code execution by visiting a photo/upload/2019/ URI. CVE ID: CVE-2019-15524	N/A	A-CSZ-CSZ 060919/272
discourse					
discourse					
Cross-Site Request Forgery (CSRF)	26-08-2019	4.3	Discourse 2.3.2 sends the CSRF token in the query string. CVE ID: CVE-2019-15515	N/A	A-DIS-DISC- 060919/273
djvulibre_pr	roject				
djvulibre					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-08-2019	4.3	In DjVuLibre 3.5.27, DjVmDir.cpp in the DJVU reader component allows attackers to cause a denial-of-service (application crash in GStringRep::strdup in libdjvu/GString.cpp caused by a heap-based buffer over-read) by crafting a DJVU file. CVE ID: CVE-2019-15142	N/A	A-DJV-DJVU- 060919/274
Uncontrolle d Resource Consumptio n	18-08-2019	4.3	In DjVuLibre 3.5.27, the bitmap reader component allows attackers to cause a denial-of-service error (resource exhaustion caused by a GBitmap::read_rle_raw infinite loop) by crafting a corrupted image file, related to libdjvu/DjVmDir.cpp and libdjvu/GBitmap.cpp. CVE ID: CVE-2019-15143	N/A	A-DJV-DJVU- 060919/275

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolle d Resource Consumptio n	18-08-2019	4.3	In DjVuLibre 3.5.27, the sorting functionality (aka GArrayTemplate <type>::sort) allows attackers to cause a denial-of-service (application crash due to an Uncontrolled Recursion) by crafting a PBM image file that is mishandled in libdjvu/GContainer.h. CVE ID: CVE-2019-15144</type>	N/A	A-DJV-DJVU- 060919/276
Out-of- bounds Read	18-08-2019	4.3	DjVuLibre 3.5.27 allows attackers to cause a denial-of-service attack (application crash via an out-of-bounds read) by crafting a corrupted JB2 image file that is mishandled in JB2Dict::JB2Codec::get_direct_con text in libdjvu/JB2Image.h because of a missing zero-bytes check in libdjvu/GBitmap.h. CVE ID: CVE-2019-15145	N/A	A-DJV-DJVU- 060919/277
domoticz					1
domoticz					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	3.5	Domoticz 4.10717 has XSS via item.Name. CVE ID: CVE-2019-15480	N/A	A-DOM- DOMO- 060919/278
easyupdates					
easy_update	s_manager				
N/A	27-08-2019	4	The stops-core-theme-and- plugin-updates plugin before 8.0.5 for WordPress has insufficient restrictions on option changes (such as disabling	N/A	A-EAS-EASY- 060919/279
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unattended theme updates)		
			because of a nonce check error.		
			CVE ID : CVE-2019-15650		
elearningfre					
insert_or_en	nbed_articula	te_con	tent		
Improper Access Control	27-08-2019	5.5	The insert-or-embed-articulate-content-into-wordpress plugin before 4.29991 for WordPress has insufficient restrictions on deleting or renaming by a Subscriber. CVE ID: CVE-2019-15648	N/A	A-ELE-INSE- 060919/280
Unrestricte d Upload of File with Dangerous Type	27-08-2019	6.5	The insert-or-embed-articulate-content-into-wordpress plugin before 4.2999 for WordPress has insufficient restrictions on file upload. CVE ID: CVE-2019-15649	N/A	A-ELE-INSE- 060919/281
ENG					
knowage					
N/A	28-08-2019	4	In Knowage through 6.1.1, an authenticated user who accesses the datasources page will gain access to any data source credentials in cleartext, which includes databases. CVE ID: CVE-2019-13348	N/A	A-ENG- KNOW- 060919/282
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	28-08-2019	4.3	In Knowage through 6.1.1, there is XSS via the start_url or user_id field to the ChangePwdServlet page. CVE ID: CVE-2019-13189	N/A	A-ENG- KNOW- 060919/283
envoyproxy				<u> </u>	

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

Weakness	Publish Date	CVSS	De	escription 8	Patch	1	NCIIPC ID		
envoy									
Uncontrolle d Resource Consumptio n	19-08-2019	5	In Envoy may confi incoming libstdc++ implement attacker ravery lord denial of seconsumpt issue to C CVE ID: 0	gure a roop path head regular entation. A may send a g URI to reservice (maion). This VE-2019-	ute to maders via the spression remote a request result in the second remory as is a relative to the second remore the second removes the second r	atch the n t with a	N/A		A-ENV- ENVO- 060919/284
eprosima									
fast-rtps									
N/A	18-08-2019	5	The Access eProsima 1.9.0 does permissic participal can lead t secure Da (DDS) par	Fast RTP: s not chec ns from r nt connect o policy b ta Distrib ctition.	S throug k partiti emote tions, wh ypass fo ution Se	N/A		A-EPR-FAST- 060919/285	
Improper Access Control	18-08-2019	5	The Access eProsima 1.9.0 allow matches we (instead of expression can lead to connection in a Data (DDS) net CVE ID: 0	plugin i S throug th patter name st nission elves), w ded en partio	N/A		A-EPR-FAST- 060919/286		
etoilewebde	sign							•	
ultimate_faq									
Improper Neutralizati	27-08-2019	4.3	The ultim	lugin be	efore	N/A		A-ETO-ULTI-	
CV Scoring Scale (CVSS)	0-1 1	-2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Des	cription 8	CVE ID		Patch	1	N	CIIPC ID
on of Input During Web Page Generation			1.8.22 for V CVE ID : CV			060	919/287			
('Cross-site Scripting')										
extenua										
silvershield										
N/A	17-08-2019	7.2	extenua Silva secure its P leading to a Escalation to attacker mu SilverShield version con user account and port for 127.0.0.1 secure its properties.	rograml Local P to SYSTE ust repla d.config. taining nt, and the rwardin ervice.	Data fold rivilege EM. The ce sqlite wi an addit nen use g to read	th a ional SSH	N/A			XT-SILV- 919/288
	•		CVE ID : CV	/E-2019	-13069					
Eyesofnetwo										
eyesofnetwo	ork									
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	16-08-2019	6.5	EyesOfNetv Remote Con shell metac module/too CVE ID : CV	mmand haracterol_all/ he	Executions in the cost field.		N/A			YE-EYES- 919/289
Facebook										
fizz										
Uncontrolle d Resource Consumptio n	20-08-2019	7.8	A peer coul handshake only paddir kept in mer handshake resulting in	be	https://w ww.faceb ook.com/ security/a dvisories/ cve-2019-			AC-FIZZ- 919/290		
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
			This issue affects versions v2019.01.28.00 and above of fizz, until v2019.08.05.00.	11924	
			CVE ID: CVE-2019-11924		
forcepoint					
next_genera	tion_firewall				
Improper Authenticat ion	20-08-2019	6.4	Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.4.x before 6.4.7, 6.5.x before 6.5.4, and 6.6.x before 6.6.2 has a serious authentication vulnerability that potentially allows unauthorized users to bypass password authentication and access services protected by the NGFW Engine. The vulnerability affects the following NGFW features when the LDAP authentication method is used as the backend authentication: IPsec VPN, SSL VPN or Browser-based user authentication. The vulnerability does not apply when any other backend authentication is used. The RADIUS authentication method is not vulnerable, for example. CVE ID: CVE-2019-6143	https://su pport.forc epoint.co m/KBArti cle?id=00 0017474	A-FOR- NEXT- 060919/291
former_proj	ect				
former					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	Former before 4.2.1 has XSS via a checkbox value. CVE ID: CVE-2019-15476	N/A	A-FOR- FORM- 060919/292
CV Scoring Scale (CVSS)	0-1 1-3	2 2	- 3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID		
fortiguard												
fortios_ips_e	engine											
Information Exposure	23-08-2019	4.3	Multiple padding oracle vulnerabilities (Zombie POODLE, GOLDENDOODLE, OpenSSL 0- length) in the CBC padding implementation of FortiOS IPS engine version 5.000 to 5.006, 4.000 to 4.036, 4.200 to 4.219, 3.547 and below, when configured with SSL Deep Inspection policies and with the IPS sensor enabled, may allow an attacker to decipher TLS connections going through the FortiGate via monitoring the traffic in a Man-in-the-middle position. CVE ID: CVE-2019-5592				https:// rtiguar om/ad ory/FG IR-19-1	d.c A-FOR- vis FORT- - 060919/2		T-		
Fortinet												
fortinac												
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	Input Durin Generation Scripting") 8.3.0 to 8.3 webUI may unauthenti perform a r	An Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") in Fortinet FortiNAC 8.3.0 to 8.3.6 and 8.5.0 admin webUI may allow an unauthenticated attacker to perform a reflected XSS attack via the search field in the webUI.				During Web Page ration ("Cross-site ting") in Fortinet FortiNAC to 8.3.6 and 8.5.0 admin I may allow an chenticated attacker to rm a reflected XSS attack via		d.c vis	A-F0 FOR 060	
gchq												
cyberchef												
Improper Neutralizati on of Input During Web Page	26-08-2019	4.3	XSS in	Chef before 8.31.2 allows operations/TextEncodingBr rce.mjs. N/A			A-GCH- CYBE- 060919/295					
CV Scoring Scale (CVSS)	0-1 1-:	2 2	3-4	3 3-4 4-5 5-6 6-7 7-8 8-9						9-10		

Weakness	Publish Date	CVSS	D	escription 8	& CVE ID		Patch		NCIIPC ID
Generation			CVE ID :	CVE-2019	-15532				
('Cross-site									
Scripting')									
Genetechsol	utions								
pie_register									
Improper									
Neutralizati									
on of			The pie-r	egister plı	ıgin befo	re			
Special			-	WordPres	_				
Elements	27-08-2019	7.5		a differen			N/A		GEN-PIE
used in an	2, 00 2017	0	CVE-2018	3-10969.			1.,11	06	0919/296
SQL			CVF ID · (CVE-2019	-15650				
Command			CVE ID.	CVE-ZUI)	-13037				
('SQL									
Injection')									
getflightpath									
flightpath									
Improper			FlightPat	h 4.8.3 has	xSS in t	he			
Neutralizati			_	Edit urgen					
on of Input			· ·	sections	_				
During Web	20-08-2019	4.3	Console.	This could	lead to	cookie	N/A		GET-FLIG-
Page			stealing a	nd other i	naliciou	S	,	06	0919/297
Generation			actions.						
('Cross-site			CVE ID :	CVE-2019	-15227				
Scripting')									
giflib_projec	t								
giflib									
				before 20					
				ed GIF file	00				
			-	-zero exce	-				
Divide By	17-08-2019	4.3		function D	_		N/A	A-	GIF-GIFL-
Zero	17-00-2017	7.3	_	if the heig			N/A	06	0919/298
			_	e data stru	icture is	equal			
			to zero.						
			CVE ID :	CVE-2019	-15133				
GNU									
libextractor									
CV Scoring Scale									

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Out-of- bounds Read	23-08-2019	4.3	GNU Libextractor through 1.9 has a heap-based buffer over-read in the function EXTRACTOR_dvi_extract_method in plugins/dvi_extractor.c. CVE ID: CVE-2019-15531	N/A	A-GNU-LIBE- 060919/299				
Gopro									
gpmf-parser	r								
Out-of- bounds Read	18-08-2019	4.3	GoPro GPMF-parser 1.2.2 has a heap-based buffer over-read (4 bytes) in GPMF_Next in GPMF_parser.c. CVE ID: CVE-2019-15146	N/A	A-GOP- GPMF- 060919/300				
Out-of- bounds Read	18-08-2019	4.3	GoPro GPMF-parser 1.2.2 has an out-of-bounds read and SEGV in GPMF_Next in GPMF_parser.c. CVE ID: CVE-2019-15147	N/A	A-GOP- GPMF- 060919/301				
Out-of- bounds Write	18-08-2019	4.3	GoPro GPMF-parser 1.2.2 has an out-of-bounds write in OpenMP4Source in demo/GPMF_mp4reader.c. CVE ID: CVE-2019-15148	N/A	A-GOP- GPMF- 060919/302				
gorm									
gorm									
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	26-08-2019	7.5	GORM before 1.9.10 allows SQL injection via incomplete parentheses. CVE ID: CVE-2019-15562	N/A	A-GOR- GORM- 060919/303				
groundhogg	groundhogg								
groundhogg	groundhogg								

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch	1	NO	CIIPC ID
Improper Control of Generation of Code ('Code Injection')	27-08-2019	6.5	The ground 1.3.5 for We admin/adm ajax.php?ad ner remote CVE ID : CV	ordPress nin- ction=bu code ex	s has wp lk_actio ecution.	n_liste	N/A		A-GF GRO 0609	
hackmd										
codimd										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	CodiMD 1.3.1, when Safari is used, allows XSS via an IFRAME element with allow-top-navigation in the sandbox attribute, in conjunction with a data: URL. CVE ID: CVE-2019-15499				N/A			AC-CODI- 019/305
httpie										
httpie										
URL Redirection to Untrusted Site ('Open Redirect')	23-08-2019	5.8	package pri vulnerable allows an a arbitrary fil filename an current dire a request fr URL pointin	All versions of the HTTPie package prior to version 1.0.3 are vulnerable to Open Redirect that allows an attacker to write an arbitrary file with supplied filename and content to the current directory, by redirecting a request from HTTP to a crafted URL pointing to a server in his or hers control.			N/A		A-H7 HTT 0609	
humanica										
humatrix_7										
Information Exposure	18-08-2019	5	The Recruit Humanica I and 1.0.0.66 unauthenti access all ca photo folde specifying a	N/A		A-HU HUM 0609				
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			and file name, such as in a recruitment_online/upload/user /[user_id]/photo/[file_name] URI.					
			CVE ID : CVE-2019-15129					
Unrestricte d Upload of File with Dangerous Type	18-08-2019	10	The Recruitment module in Humanica Humatrix 7 1.0.0.203 and 1.0.0.681 allows an unauthenticated attacker to upload any file type to a candidate's profile picture folder via a crafted recruitment_online/personalData /act_personaltab.cfm multiple-part POST request with a predictable WRC01_USERID parameter. Moreover, the attacker can upload executable content (e.g., asp or aspx) for executing OS commands on the server. CVE ID: CVE-2019-15130	N/A	A-HUM- HUMA- 060919/308			
IBM								
mq_applian	ce							
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	20-08-2019	7.2	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.6, 7.6.0.0 through 7.6.0.15 and IBM MQ Appliance 8.0.0.0 through 8.0.0.12, 9.1.0.0 through 9.1.0.2, and 9.1.1 through 9.1.2 could allow a local attacker to execute arbitrary commands on the system, caused by a command injection vulnerability. IBM X- Force ID: 16188. CVE ID: CVE-2019-4294	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 58933	A-IBM- MQ_A- 060919/309			
storediq								
Cross-Site	20-08-2019	4.3	IBM StoredIQ 7.6.0 is vulnerable	N/A	A-IBM-STOR-			
CV Scoring Scale (CVSS)	0-1 1-7	2 2	101 3-4 4-5 5-6 6-7	7-8	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 158700. CVE ID: CVE-2019-4167		060919/310
informix_dy	namic_server				
N/A	20-08-2019	7.2	IBM Informix Dynamic Server Enterprise Edition 12.1 could allow a local privileged Informix user to load a malicious shared library and gain root access privileges. IBM X-Force ID: 159941.	N/A	A-IBM-INFO- 060919/311
datanawan	ratovyov		CVE ID : CVE-2019-4253		
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	20-08-2019	7.2	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.6, 7.6.0.0 through 7.6.0.15 and IBM MQ Appliance 8.0.0.0 through 8.0.0.12, 9.1.0.0 through 9.1.0.2, and 9.1.1 through 9.1.2 could allow a local attacker to execute arbitrary commands on the system, caused by a command injection vulnerability. IBM X- Force ID: 16188. CVE ID: CVE-2019-4294	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 58933	A-IBM- DATA- 060919/312
emptoris_so	urcing				
Information Exposure	20-08-2019	4	IBM Emptoris Sourcing 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 could allow an authenticated user to obtain sensitive information from error messages IBM X-Force	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm108 80221	A-IBM- EMPT- 060919/313
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	cvss	Desc	ription 8	CVE ID		Patch	1	N	CIIPC ID
			ID: 161034.	ı						
			CVE ID : CV	E-2019	-4308					
Information Exposure	20-08-2019	4	IBM Emptor through 10. Managemer 10.1.3, and Analysis 10 generates a includes ser that could b attacks agai X-Force ID:	https://ww.ibn om/sup ort/dod ew.wss d=ibm1 80221	n.c pp cvi ?ui	A-IE EMI 060				
Information Exposure	20-08-2019	4	IBM Emptoris Sourcing 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164069.				https://www.ibmom/suport/dodew.wssd=ibm180221	n.c pp cvi ?ui	A-IE EMI 060	
emptoris_sp	end_analysis									
Information Exposure	20-08-2019	4	IBM Emptoris Sourcing 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 could allow an authenticated user to obtain sensitive information from error messages IBM X-Force ID: 161034.			through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 could allow an authenticated user to obtain sensitive information from error messages IBM X-Force ID: 161034. https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm108		n.c pp cvi ?ui	A-IE EMI 060	
Improper Neutralizati on of	20-08-2019	7.5	through 10.	IBM Contract Management 10.1.0 https://w through 10.1.3 and IBM Emptoris www.ibm.c Spend Analysis 10.1.0 through om/supp		n.c	A-IE EMI 060			
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		10.1.3 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the backend database. IBM X-Force ID: 164064. CVE ID: CVE-2019-4481	ort/docvi ew.wss?ui d=ibm108 80223	
20-08-2019	3.5	IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 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: 164066. CVE ID: CVE-2019-4482	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm108 80217	A-IBM- EMPT- 060919/318
20-08-2019	7.5	IBM Contract Management 10.1.0 through 10.1.3 and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the backend database. IBM X-Force ID: 164067. CVE ID: CVE-2019-4483	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm108 80223	A-IBM- EMPT- 060919/319
20-08-2019	4	IBM Emptoris Sourcing 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 generates an error message that includes sensitive information	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm108 80221	A-IBM- EMPT- 060919/320
	20-08-2019	20-08-2019 7.5	injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the backend database. IBM X-Force ID: 164064. CVE ID: CVE-2019-4481 IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 is vulnerabile 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: 164066. CVE ID: CVE-2019-4482 IBM Contract Management 10.1.0 through 10.1.3 and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the backend database. IBM X-Force ID: 164067. CVE ID: CVE-2019-4483 IBM Emptoris Sourcing 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 generates an error message that	injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the backend database. IBM X-Force ID: 164064. CVE ID: CVE-2019-4481 IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 is vulnerable to cross-site scripting. This vulnerablity 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: 164066. CVE ID: CVE-2019-4482 IBM Contract Management 10.1.0 through 10.1.3 and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the backend database. IBM X-Force ID: 164067. CVE ID: CVE-2019-4483 IBM Emptoris Sourcing 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 generates an error message that deibm108

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			that could be used in further attacks against the system. IBM X-Force ID: 164068. CVE ID: CVE-2019-4484		
Information Exposure	20-08-2019	4	IBM Emptoris Sourcing 10.1.0 through 10.1.3, IBM Contract Management 10.1.0 through 10.1.3, and IBM Emptoris Spend Analysis 10.1.0 through 10.1.3 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164069.	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm108 80221	A-IBM- EMPT- 060919/321
security gua	rdium_big_da	ata inte			
N/A	20-08-2019	5	IBM Security Guardium Big Data Intelligence 4.0 (SonarG) uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 161036. CVE ID: CVE-2019-4310	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 60298	A-IBM-SECU- 060919/322
Uncontrolle d Resource Consumptio n	20-08-2019	5	IBM Security Guardium Big Data Intelligence 4.0 (SonarG) does not properly restrict the size or amount of resources that are requested or influenced by an actor. This weakness can be used to consume more resources than intended. IBM X-Force ID: 161417. CVE ID: CVE-2019-4338	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 60858	A-IBM-SECU- 060919/323
Improper Restriction of XML External	20-08-2019	6.4	IBM Security Guardium Big Data Intelligence 4.0 (SonarG) is vulnerable to an XML External Entity Injection (XXE) attack	https://w ww.ibm.c om/supp ort/docvi	A-IBM-SECU- 060919/324

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
Entity Reference ('XXE')			when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 161419.	ew.wss?ui d=ibm109 60856				
			CVE ID: CVE-2019-4340					
infosphere_	global_name_	manag	ement					
Improper Restriction of XML External Entity Reference ('XXE')	20-08-2019	6.4	IBM InfoSphere Global Name Management 5.0 and 6.0 and IBM InfoSphere Identity Insight 8.1 and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 162890.	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 58081	A-IBM-INFO- 060919/325			
			CVE ID : CVE-2019-4433					
infosphere_	identity_insig	ht						
Improper Restriction of XML External Entity Reference ('XXE')	20-08-2019	6.4	IBM InfoSphere Global Name Management 5.0 and 6.0 and IBM InfoSphere Identity Insight 8.1 and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 162890. CVE ID: CVE-2019-4433		A-IBM-INFO- 060919/326			
security_acc	cess_manager_	_for_en	terprise_single_sign-on					
Improper Restriction of XML External	26-08-2019	6.4	IBM Security Access Manager for Enterprise Single Sign-On 8.2.2 is vulnerable to an XML External Entity Injection (XXE) attack A-IBM-SEC 060919/32					
CV Scoring Scale (CVSS)	e 0-1 1-3	2 2	- 3 3-4 4-5 5-6 6-7	7-8	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference ('XXE')			when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 164555.		
			CVE ID : CVE-2019-4513		
api_connect					l .
Improper Input Validation	20-08-2019	5	IBM API Connect 2018.1 through 2018.4.1.6 developer portal could allow an unauthorized user to cause a denial of service via an unprotected API. IBM X-Force ID: 162263. CVE ID: CVE-2019-4402	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 58193	A-IBM-API 060919/328
Information Exposure	20-08-2019	5	IBM API Connect 2018.1 through 2018.4.1.6 may inadvertently leak sensitive details about internal servers and network via API swagger. IBM X-force ID: 162947.	N/A	A-IBM-API 060919/329
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-08-2019	5	IBM API Connect 5.0.0.0 through 5.0.8.6 developer portal 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: 163681. CVE ID: CVE-2019-4460	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 60848	A-IBM-API 060919/330
intelligent_o	perations_ce	nter			
Improper Restriction of XML External	20-08-2019	6.4	IBM Intelligent Operations Center V5.1.0 through V5.2.0 is vulnerable to an XML External Entity Injection (XXE) attack	https://w ww.ibm.c om/supp ort/docvi	A-IBM-INTE- 060919/331
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference ('XXE')			when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 162737.	ew.wss?ui d=ibm109 56433	
			CVE ID: CVE-2019-4419		
Information Exposure	20-08-2019	2.1	IBM Intelligent Operations Center V5.1.0 through V5.2.0 could disclose detailed error messages, revealing sensitive information that could aid in further attacks against the system. IBM X-Force ID: 162738. CVE ID: CVE-2019-4420	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 56429	A-IBM-INTE- 060919/332
intelligent_operations_center_for_emergency_management					
Improper Restriction of XML External Entity Reference ('XXE')	20-08-2019	6.4	IBM Intelligent Operations Center V5.1.0 through V5.2.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 162737.	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 56433	A-IBM-INTE- 060919/333
			CVE ID : CVE-2019-4419		
Information Exposure	20-08-2019	2.1	IBM Intelligent Operations Center V5.1.0 through V5.2.0 could disclose detailed error messages, revealing sensitive information that could aid in further attacks against the system. IBM X-Force ID: 162738. CVE ID: CVE-2019-4420	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 56429	A-IBM-INTE- 060919/334
water_operations_for_waternamics					
Improper Restriction	20-08-2019	6.4	IBM Intelligent Operations Center V5.1.0 through V5.2.0 is	https://w ww.ibm.c	A-IBM- WATE-
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4 4-5 5-6 6-7	7-8	3-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
of XML External Entity Reference ('XXE')			vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 162737. CVE ID: CVE-2019-4419	om/supp ort/docvi ew.wss?ui d=ibm109 56433	060919/335
Information Exposure	20-08-2019	2.1	IBM Intelligent Operations Center V5.1.0 through V5.2.0 could disclose detailed error messages, revealing sensitive information that could aid in further attacks against the system. IBM X-Force ID: 162738. CVE ID: CVE-2019-4420	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 56429	A-IBM- WATE- 060919/336
business_au	tomation_wo	rkflow			
Improper Restriction of XML External Entity Reference ('XXE')	20-08-2019	6.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, and 19.0.0.2 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 162770.	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 59537	A-IBM-BUSI- 060919/337
			CVE ID : CVE-2019-4424		
Information Exposure	20-08-2019	3.5	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, and 18.0.0.2 could allow a user to obtain highly sensitive information from another user by inserting links that would be clicked on by unsuspecting users. IBM X-Force ID: 162771.	https://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=ibm109 59261	A-IBM-BUSI- 060919/338

Weakness	Publish Date	CVSS	Des	scription 8	CVE ID		Patch		NCIIPC ID							
			CVE ID : C	VE-2019	-4425											
business_pr	ocess_manage	er														
Improper Restriction of XML External Entity Reference ('XXE')	20-08-2019	6.4	IBM Busine Workflow 18.0.0.2, 19 vulnerable Entity Injection when procremote attaininformation resources. 162770.	18.0.0.0, 9.0.0.1, and to an XM essing XM acker country to expense of the total marker to the total marker to expense of the total marker to expense of the total marker total	18.0.0.1 and 19.0. IL Exter E) attac ML data. ald explo ose sens sume me	0.2 is nal k A oit this sitive	https://w ww.ibm.c om/supp ort/docvi ew.wss?u d=ibm109 59537	A- 06	·IBM-BUSI- 50919/339							
			IBM Busine													
Information Exposure	20-08-2019	Workflow 18.0.0.0, 18.0.0.1, and 18.0.0.2 could allow a user to obtain highly sensitive							18.0.0.2 could allow a user to obtain highly sensitive om/ort/ort/ort/ort/ort/ort/ort/ort/ort/ort					https://www.ibm.com/support/docview.wss?ud=ibm10959261	A- 06	IBM-BUSI- 50919/340
			CVE ID : CV	VE-2019	-4425											
cloud_privat	e															
Cross-Site Request Forgery (CSRF)	20-08-2019	6.8	is vulnerab forgery wh attacker to unauthoriz from a use trusts. IBM	IBM Cloud Private 3.1.1 and 3.1.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 158116. CVE ID: CVE-2019-4117			N/A	CI	IBM- LOU- 50919/341							
Improper Neutralizati on of Input During Web Page Generation	20-08-2019	3.5	IBM Cloud is vulnerab scripting. T allows used JavaScript thus alteria	ole to cro This vulners to emb code in the	ss-site erability oed arbit he Web	rary	N/A	CI	IBM- LOU- 50919/342							
CV Scoring Scale	0-1 1-:		3-4	4-5	5-6	6-7	7-8	8-9	9-10							

(CVSS)

Weakness	Publish D	ate	CVSS		Des	cription 8	CVE ID		Patch	1	N	CIIPC ID
('Cross-site Scripting')				to d	ctionalit credentia sted sess 3146.	als discl	osure w	ithin a				
				CV	E ID : CV	E-2019	-4120					
Igniterealtin	ne											
openfire												
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-20)19	4.3	4.4 LD	ite Realt 1 has re AP setup E ID : CV	KSS via a	N/A			GN-OPEN- 919/343		
imagely												
nextgen_gall	ery											
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	27-08-20)19	7.5	exis Gal Wo exp wo exe on mo /pa _dis	A SQL injection vulnerability exists in the Imagely NextGEN Gallery plugin before 3.2.10 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via modules/nextgen_gallery_display /package.module.nextgen_gallery_display.php. CVE ID: CVE-2019-14314				N/A		A-IN NEX 060	
Imagemagic	k											
imagemagic	k											
Out-of- bounds Read	18-08-20)19	4.3	The XWD image (X Window System window dumping file) parsing component in ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (application crash resulting from an out-of-bounds					N/A		A-IN IMA 060	
CV Scoring Scale (CVSS)	0-1	1-2	2	2-3 3-4 4-5 5-6 6-7				6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	D	escription 8	& CVE ID		Patch		NCIIPC ID				
			Read) in coders/x corrupted different 2019-114	wd.c by cr l XWD im vulnerabi	afting a	a							
			CVE ID :	CVE-2019	-15139								
Use After Free	18-08-2019	6.8	7.0.8-43 (attackers service (u application have unsp crafting a mishandl MagickCo	coders/mat.c in ImageMagick 7.0.8-43 Q16 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by crafting a Matlab image file that is mishandled in ReadImage in MagickCore/constitute.c. CVE ID: CVE-2019-15140				7.0.8-43 Q16 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by crafting a Matlab image file that is mishandled in ReadImage in MagickCore/constitute.c.				I	A-IMA- MAG- 060919/346
Out-of- bounds Read	18-08-2019	4.3	WriteTIF in ImageN allows att denial-of- crash res based but crafted T TIFFRew TIFFWrit TIFFWrit in tif_dirv this occur incomple 11597.	FImage in Aggick 7.0 ackers to service (aulting from FF image riteDirectory eDirectory rite.c of Its because te fix for 0	coders/ cause a applicati n a heap read) via file, rela ory, y y Sec, and y TagColo ibTIFF.	N/A	I	A-IMA- MAG- 060919/347					
impress													
givewp													
Improper Neutralizati on of Input During Web Page	22-08-2019	3.5	The give plugin before 2.4.7 for WordPress has XSS via a donor name. CVE ID: CVE-2019-15317			WordPress has XSS via a donor name.		onor	N/A		A-IMP-GIVE- 060919/348		
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	5-6	6-7	7-8	8-9	9-10					

Weakness	Publish Date	cvss		Description 8	& CVE ID		Patch	n	N	CIIPC ID
Generation ('Cross-site Scripting')										
instamojo										
payment_ga	teway									
Improper Input Validation	29-08-2019	5	WooCon Payment WordPre Tamperi as demo an item i	y//amounderce Instance Inst	tamojo olugin 1.0 Parameto gn paran purchan nan the	er neter,	N/A			IS-PAYM- 919/349
Intel										
authenticate	9									
N/A	19-08-2019	4.6	Imprope software Authenti allow an potentia privilege CVE ID:	https:/ ww.into om/con nt/www us/en/ urity- center/ visory/ el-sa- 00275. ml	el.c nte w/ sec /ad /int	A-IN AUT 060				
remote_disp	lays_sdk									
N/A	19-08-2019	4.6	Imprope installer Displays R2 may a user to p escalation access. CVE ID:	e n 2.0.1 ted	https://www.intom/cont/www.us/en/urity-center/visory/el-sa-00277.	el.c nte w/ sec /ad /int	A-IN REM 060			
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ml	
processor_id	lentification_	utility			
Improper Access Control	19-08-2019	4.6	Insufficient access control in a hardware abstraction driver for Intel(R) Processor Identification Utility for Windows before version 6.1.0731 may allow an authenticated user to potentially enable escalation of privilege, denial of service or information disclosure via local access. CVE ID: CVE-2019-11163	https://w ww.intel.c om/conte nt/www/ us/en/sec urity- center/ad visory/int el-sa- 00281.ht ml	A-INT-PROC- 060919/352
raid_web_co	nsole_2				
Improper Authenticat ion	19-08-2019	5.8	Authentication bypass in the web console for Intel(R) Raid Web Console 2 all versions may allow an unauthenticated attacker to potentially enable disclosure of information via network access. CVE ID: CVE-2019-0173	https://w ww.intel.c om/conte nt/www/ us/en/sec urity- center/ad visory/int el-sa- 00246.ht ml	A-INT-RAID- 060919/353
jc21					
nginx_proxy	_manager				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-08-2019	4.9	jc21 Nginx Proxy Manager before 2.0.13 allows %2e%2e%2f directory traversal. CVE ID: CVE-2019-15517	N/A	A-JC2-NGIN- 060919/354
Jenkins					
splunk					
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7 114	7-8	9-10

Weakness	Publish Date	cvss		Des	cription 8	& CVE ID		Patch	NCIIPC ID
Improper Input Validation	28-08-2019	6.5	Jeni ear Ove pro HT' arb	kins Splilier allowerall/Revide a G FP endpitrary cokins man	bypass vunk Plugwed atta ad permatroovy so oint that ode exectster JVM	gin 1.7.4 ckers w ission to cript to a t can res ution or	and ith o an sult in	N/A	EN-SPLU- 0919/355
jooby									
jooby									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	defa	ault erro	e 1.6.4 f or handl E-2019	er.	N/A	00-J00B- 0919/356	
Kaseya									
virtual_syste	em_administ	rator							
Information Exposure	26-08-2019	7.8	Kas Adr 9.4. info vuli atta forr app sen For dire rep con suc Act	eya Virt ministra 0.37. It ormation nerabilit acker can matted ra lication sitive fil example example ectory can orts. Be tains the h as NM ive Dire	as discovered and series and dovered and dovered and series and dovered and series and s	em A) throughtical cure hauthent roperly to the windoad informat DATARE right direct s of repoints h Status main ter can e	N/A	KAS-VIRT- 0919/357	
			coll	ect this	critical i	nformat	ion		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and parse it for information. There are a number of directories affected.		
			CVE ID : CVE-2019-15506		
kbpublisher					
kbpublisher					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	21-08-2019	7.5	KBPublisher 6.0.2.1 has SQL Injection via the admin/index.php?module=report entry_id[0] parameter, the admin/index.php?module=log id parameter, or an index.php?View=print&id[]= request. CVE ID: CVE-2019-10687	N/A	A-KBP- KBPU- 060919/358
kbrw					
sweet_xml					
Improper Restriction of XML External Entity Reference ('XXE')	19-08-2019	5	The SweetXml (aka sweet_xml) package through 0.6.6 for Erlang and Elixir allows attackers to cause a denial of service (resource consumption) via an XML entity expansion attack with an inline DTD. CVE ID: CVE-2019-15160	N/A	A-KBR- SWEE- 060919/359
Kunena					
kunena					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-08-2019	4.3	The Kunena extension before 5.1.14 for Joomla! allows XSS via BBCode. CVE ID: CVE-2019-15120	N/A	A-KUN- KUNE- 060919/360
laracom					·
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS		Desc	ription 8	CVE ID		Patch		NCIIPC ID
laracom			•							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	26-08-2019	4.3	Comm search	erce : ?q= X	Softwar KSS.	el FREE e) 1.4.11 - 15489	l has	N/A	I	A-LAR- LARA- 060919/361
Lenovo										
solution_cen	ter									
Information Exposure	21-08-2019	7.5	Lenove 03.12.0 support be write location privile ended Solution recome migrate Lenove	o Solu 003, v rted, tten t ons, p ege es supp on Ce menc te to I o Dias	ution Ce which is could al co non-s otential calation ort for I nter and led that	l custom Vantage in April	https://si pport.lend vo.com/s olutions/ LEN- 27811		A-LEN- SOLU- D60919/362	
librenms										
librenms										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	28-08-2019	3.5	Create Device Create Templ consol stealin actions exploid	User e, Not Mair ate se e. Thi ig and s. Thi ted w nt.	, Invent ification itenance ections of is could l other i s vulner ith an a	s XSS in ory, Add s, Alert e, and Al of the ad lead to e maliciou rability cuthentic	Rule, ert min cookie s can be	N/A		A-LIB-LIBR- 060919/363
Live555										
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Des	cription 8	CVE ID		Patch	1	N	CIIPC ID
streaming_n	nedia										
Use After Free	19-08-2019	7.5	Use Gen lien the suc by t	-After-Facilities -After-Facil	fore 201 Free becandiaServen WithId ient sessa which is G10r2 and iplexors.	nuse r::create can gen sion ID is s mishar nd Matr	eNewC erate n ndled	N/A			V-STRE- 919/364
Lsoft											
listserv											
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	26-08-2019	4.3	Reflected cross site scripting (XSS) in L-Soft LISTSERV before 16.5-2018a exists via the /scripts/wa.exe OK parameter. CVE ID: CVE-2019-15501					N/A			50-LIST- 919/365
manageyour	rteam	_									
myt_project	_managemen	t									
Cross-Site Request Forgery (CSRF)	28-08-2019	6.8	lack exa CSR atta adn arb	MyT Project Management 1.5.1 lacks CSRF protection and, for example, allows a user/create CSRF attack. This could lead to an attacker tricking the administrator into executing arbitrary code via a specially crafted HTML page. CVE ID: CVE-2019-15496			for ate d to an g ly	N/A		MY	AN- Γ 919/366
Mcafee											
data_loss_pr	evention_en	lpoint									
Improper Restriction of Operations	21-08-2019	4.9	Los Wir	s Preve ndows 1	flow in l ntion (D 1.x prion l user to	LPe) for r to 11.3	.2.8	https:// .mcafee m/corp ate/ind	e.co oor	A-M DAT 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	2-3 3-4 4-5 5-6 6-					8	-9	9-10

Weakness	Publish Date	cvss		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
within the Bounds of a Memory Buffer			"blucon DLI inte	ue scree structed Pe which ernal cho Pe readi mory.	perating n" via a of the message the bypass the bypass the cks and the message the bypass the cks and the characteristics the	carefully ge sent t es DLPe results ocated	/ O	?page= ntent&i SB1029	id=		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-08-2019	4.9	Los Win allo Win "blu me: who	s Preventions 1 sows local andows of the scree ssage seen decryding una	flow in Intion (D) 1.x prion I user to perating n" via an ont to DL opted reseallocated 7E-2019	LPe) for to 11.3 cause the graph of the grap	.2.8 ne to ted h	https:// .mcafee m/corp ate/ind ?page= ntent&i	e.co oor lex co id=	A-M DAT 060	_
Microfocus											
verastream_	host_integra	to									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-08-2019	5	Mic Inte and allo atta	h traver ero Focu egrator (l earlier, ows rem ackers to	ream Ho ersions 7 nerabili othentica bitrary	https://pport.n rofocus m/kb/o .php?id 024061	nic s.co doc =7	A-M VER 060			
content_mar	nager										
Information Exposure	30-08-2019	4	Foo 9.1, who dat use sub nor	cus Cont , 9.2 and en confi abase, a rs to gai set of re mally be	n exposuent Man 9.3. Thi gured to llows va n access cords the able to is in an	ager, vers vulner use and lid systems to a lim access vers	rsions rability Oracle em nited ld not when	https:// ftwares port.so: aregrp. m/doc/ M0349 82	sup ftw co /K	A-M CON 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch	1	NCIIP	CID
			abnormal s	tate.						
			CVE ID : CV	/E-2019	-11658					
micropyram	iid									
django_crm										
Cross-Site Request Forgery (CSRF)	27-08-2019	6.8	Multiple CS MicroPyrar via /change admin/, /a /cases/cre password-l /comment /document /document /login/.	mid Djan e-passwo pi/settin ate/, /ch py-admin /add/, s/1/viev s/create	go CRM ord-by- gs/add, ange- n/, w/,	0.2.1	N/A		A-MIC-I 060919	•
			CVE ID : CV	/E-2019	-11457					
mirasys										
mirasys_vms	S									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-08-2019	5	Mirasys VM 8.x before V Download(AutoUpdat SMServer.e Directory T could use iterate over system file without pro This includ backups, W might caus confidentia	78.3.2 m) methode Service on the service of the se	ishandle d of in ng to . An atta iis meth interest wnload ithentic database g files, e us impa	es the acker od to ing them ation. e tc. and ct on	N/A	I	A-MIR- MIRA- 060919	/372
Deserializat ion of Untrusted	22-08-2019	10	Mirasys VM 8.x before V Mirasys.Co ataCrypt m	IS before /8.3.2 m mmon.U	e V7.6.1 ishandle tils.Secu	and es the irity.D	N/A	I	A-MIR- MIRA- 060919	/373
Data			in AuditTra							
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9	9-10

Weakness	Publish Date	cvss	Des	scription 8	& CVE ID		Patch)	N	CIIPC ID
			SMServer triggers in within the in which a serialized executed v The attack encrypt th hardcoded	secure do .NET gar gadget (object) m vith SYST er must p e object; keys are	eserialize bage contained and be TEM prive properly howeve	ation llector, ed in a rileges. r, the le.				
Unrestricte d Upload of File with Dangerous Type	22-08-2019	10	Mirasys VI 8.x before auto-upda IDVRUpda DVRServer upload file action, and files with S	N/A		A-M MIR 060				
mixin-deep_	project									
mixin-deep										
Argument Injection or Modificatio n	23-08-2019	7.5	mixin-dee Prototype before 1.3. The function tricked interproperties using a con	Pollutior 2 and ve on mixin o adding of Objec	n in vers rsion 2.0 -deep co or modi t.prototy	ions 0.0. ould be ifying ype l.	N/A			IIX-MIXI- 919/375
my_calendar	 r_project									
my_calendar	r									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	28-08-2019	4.3	The my-ca 3.1.10 for 'CVE ID : C'	N/A			IYMY_C- 919/376			
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4 4-5 5-6 6-7 7-8 8-9 9						9-10	

Weakness	Publish Dat	e CVSS		Des	cription 8	k CVE ID		Patch	1	NCIIPC ID
Scripting')										
Ncrafts										
formcraft										
Cross-Site Request Forgery (CSRF)	16-08-201	9 6.8	plu has	e formcr igin befo s CSRF. E ID : CV	re 1.2.2	for Wor	dPress	N/A	F	-NCR- ORM- 60919/377
ncurses_pro	ject									
ncurses										
Use of Externally- Controlled Format String	26-08-201	9 6.4	ncu Ru issi bed mi	An issue was discovered in the ncurses crate through 5.99.0 for Rust. There are format string issues in printw functions because C format arguments are mishandled. CVE ID: CVE-2019-15547					N	-NCU- CUR- 60919/378
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-08-201	9 7.5	ncu Ru mv bed fur	An issue was discovered in the ncurses crate through 5.99.0 for Rust. There are instr and mvwinstr buffer overflows because interaction with C functions is mishandled. CVE ID: CVE-2019-15548				N/A	N	-NCU- CUR- 60919/379
networkgen	omics									
mitogen										
N/A	18-08-201	9 6.8	Mintha routh the by extended the control of the con	** DISPUTED ** core.py in Mitogen before 0.2.8 has a typo that drops the unidirectional- routing protection mechanism in the case of a child that is initiated by another child. The Ansible extension is unaffected. NOTE: the vendor disputes this issue because it is exploitable only in conjunction with hypothetical other factors, i.e., an affected use				N/A	M	-NET- ITO- 60919/380
					,,					
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			case within a library caller, and a bug in the message receiver policy code that led to reliance on this extra protection mechanism. CVE ID: CVE-2019-15149		
nltk					
nltk					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-08-2019	5	NLTK Downloader before 3.4.5 is vulnerable to a directory traversal, allowing attackers to write arbitrary files via a/ (dot dot slash) in an NLTK package (ZIP archive) that is mishandled during extraction. CVE ID: CVE-2019-14751	N/A	A-NLT- NLTK- 060919/381
nokogiri_pr	oject				
nokogiri					
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	16-08-2019	7.5	A command injection vulnerability in Nokogiri v1.10.3 and earlier allows commands to be executed in a subprocess via Ruby's `Kernel.open` method. Processes are vulnerable only if the undocumented method `Nokogiri::CSS::Tokenizer#load_fi le` is being called with unsafe user input as the filename. This vulnerability appears in code generated by the Rexical gem versions v1.0.6 and earlier. Rexical is used by Nokogiri to generate lexical scanner code for parsing CSS queries. The underlying vulnerability was addressed in Rexical v1.0.7 and Nokogiri upgraded to this version of Rexical in Nokogiri v1.10.4.	N/A	A-NOK- NOKO- 060919/382

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Desc	cription &	CVE ID		Patcl	h	NCIIF	PC ID
			CVI	E ID : CV	E-2019	-5477					
nps_project									·		
nps											
N/A	5.8	lib/install/install.go in cnlh nps through 0.23.2 uses 0777 permissions for /usr/local/bin/nps and/or /usr/bin/nps, leading to a file overwrite by a local user. CVE ID: CVE-2019-15119				N/A		A-NPS- 060919			
obdev											
little_snitch											
N/A	23-08-2019	4.9	Little Snitch versions 4.3.0 to 4.3.2 have a local privilege escalation vulnerability in their privileged helper tool. The privileged helper tool implements an XPC interface which is available to any process and allows directory listings and copying files as root.				N/A		A-0BD 060919		
N/A	23-08-2019	4.9	Little Snitch versions 4.4.0 fixes a vulnerability in a privileged helper tool. However, the operating system may have made a copy of the privileged helper which is not removed or updated immediately. Computers may therefore still be vulnerable after upgrading to 4.4.0. Version 4.4.1 fixes this issue by removing the operating system's copy during the upgrade. CVE ID: CVE-2019-13014				N/A		A-OBD 060919		
octopus											
server											
CV Scoring Scale											

Weakness	Publish Date	cvss	Des	cription 8	Patch	n 1	NCIIPC ID			
Information Exposure Through Log Files	23-08-2019	3.5	In Octopus 2018.8.4 to request pro authentical limited spe circumstan deploymen request pro deploymen is fixed in 2 back-porte well as LTS	2019.7. oxy is conted user ecial-charactes) count that we oxy passive to LTS and to LTS and 2019.3.	6, when nfigured (in certar racters ld triggerites the word to cleartext 7he fix 2019.6.	a web I, an ain er a web the This was 7 as	N/A		OCT-SERV- 0919/386	
Information Exposure Through Log Files	23-08-2019	3.5	In Octopus 3.0.8 to 5.0 proxy is co authentical limited Oct circumstan deploymen request pro deploymen is fixed in 5 ported to 4 CVE ID : CV	a web r , an (in certant antVariable Id trigge rites the word to cleartext	N/A		OCT-SERV- 0919/387			
octopus_dep	oloy									
Information Exposure	27-08-2019	4	In Octopus through 20 circumstan user with V permission values. This	19.7.9, inces, an avariable variable va	n certain uthentio liew view sen in 2019	N/A	OC	OCT- TO- O919/388		
ohdsi										
webapi										
Improper Neutralizati on of	26-08-2019	7.5	Observational Health Data Sciences and Informatics (OHDSI) WebAPI before 2.7.2 allows SQL					WE	A-OHD- WEBA- 060919/389	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command			injection in FeatureExtractionService.java. CVE ID: CVE-2019-15563		
Command ('SQL Injection')					
omg					
dds_security					
Information Exposure	18-08-2019	5	The handshake protocol in Object Management Group (OMG) DDS Security 1.1 sends cleartext information about all of the capabilities of a participant (including capabilities inapplicable to the current session), which makes it easier for attackers to discover potentially sensitive reachability information on a Data Distribution Service (DDS) network. CVE ID: CVE-2019-15135	N/A	A-OMG- DDS 060919/39
Open-emr					
openemr					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	4.3	In OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the patient_id parameter. This could allow an attacker to execute arbitrary code in the context of a user's session. CVE ID: CVE-2019-3963	N/A	A-OPE- OPEN- 060919/39
Improper Neutralizati on of Input During Web Page	20-08-2019	4.3	In OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the doc_id parameter. This could allow an attacker to execute	N/A	A-OPE- OPEN- 060919/39
CV Scoring Scale	0-1 1-2		-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			arbitrary code in the context of a user's session. CVE ID: CVE-2019-3964		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	4.3	In OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the document_id parameter. This could allow an attacker to execute arbitrary code in the context of a user's session. CVE ID: CVE-2019-3965	N/A	A-OPE- OPEN- 060919/393
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	4.3	In OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the foreign_id parameter. This could allow an attacker to execute arbitrary code in the context of a user's session. CVE ID: CVE-2019-3966	N/A	A-OPE- OPEN- 060919/394
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-08-2019	4	In OpenEMR 5.0.1 and earlier, the patient file download interface contains a directory traversal flaw that allows authenticated attackers to download arbitrary files from the host system. CVE ID: CVE-2019-3967	N/A	A-OPE- OPEN- 060919/395
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	20-08-2019	9	In OpenEMR 5.0.1 and earlier, an authenticated attacker can execute arbitrary commands on the host system via the Scanned Forms interface when creating a new form. CVE ID: CVE-2019-3968	N/A	A-OPE- OPEN- 060919/396
openpgpjs					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	N	ICIIPC ID
openpgpjs						
Improper Verification of Cryptograp hic Signature	22-08-2019	5	Improper Verification of a Cryptographic Signature in OpenPGP.js <=4.1.2 allows an attacker to forge signed messages by replacing its signatures with a "standalone" or "timestamp" signature. CVE ID: CVE-2019-9153	N/A	A-0 OPF 060	
Improper Verification of Cryptograp hic Signature	22-08-2019	5	Improper Verification of a Cryptographic Signature in OpenPGP.js <=4.1.2 allows an attacker to pass off unsigned data as signed. CVE ID: CVE-2019-9154	N/A	A-0 OPI 060	
N/A	22-08-2019	4.3	A cryptographic issue in OpenPGP.js <=4.2.0 allows an attacker who is able provide forged messages and gain feedback about whether decryption of these messages succeeded to conduct an invalid curve attack in order to gain the victim's ECDH private key. CVE ID: CVE-2019-9155	N/A	A-0 OPI 060	
openweave						
openweave-	core					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	6.8	An exploitable command execution vulnerability exists in the print-tly command of Weave tool. A specially crafted weave TLV can trigger a stack-based buffer overflow, resulting in code execution. An attacker can trigger this vulnerability by convincing the user to open a specially crafted Weave command. CVE ID: CVE-2019-5038	N/A	A-0 OPF 060	
CV Scoring Scale (CVSS)	9 0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-08-2019	6.8	An exploitable command execution vulnerability exists in the ASN1 certificate writing functionality of Openweave-core version 4.0.2. A specially crafted weave certificate can trigger a heap-based buffer overflow, resulting in code execution. An attacker can craft a weave certificate to trigger this vulnerability. CVE ID: CVE-2019-5039	N/A	A-OPE- OPEN- 060919/401
Integer Overflow or Wraparoun d	20-08-2019	5	An exploitable information disclosure vulnerability exists in the Weave MessageLayer parsing of Openweave-core version 4.0.2 and Nest Cam IQ Indoor version 4620002. A specially crafted weave packet can cause an integer overflow to occur, resulting in PacketBuffer data reuse. An attacker can send a packet to trigger this vulnerability. CVE ID: CVE-2019-5040	N/A	A-OPE- OPEN- 060919/402
openwrt					
libuci					
Improper Input Validation	23-08-2019	7.8	An issue was discovered in OpenWrt libuci (aka Library for the Unified Configuration Interface) as used on Motorola CX2L MWR04L 1.01 and C1 MWR03 1.01 devices. /tmp/.uci/network locking is mishandled after reception of a long SetWanSettings command, leading to a device hang. CVE ID: CVE-2019-15513	N/A	A-OPE-LIBU- 060919/403

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Des	cription &	CVE ID		Patch	l	N	CIIPC ID
Open-xchan	ge									
open-xchang	ge_appsuite									
Improper Input Validation	20-08-2019	5.8	OX App Sui Content Sp CVE ID : CV	oofing.			N/A		A-0 OPE 060	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	3.5	OX App Sui allows XSS. CVE ID : CV		N/A		A-0 OPE 060			
N/A	20-08-2019	2.1	OX App Sui has Insecur CVE ID : CV	ssions.	N/A		A-0 OPE 060			
optiontree_project										
optiontree										
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component ('Injection')	22-08-2019	7.5	The option 2.7.0 for W Injection by nonce.	N/A			PT-OPTI- 919/407			
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m	22-08-2019	7.5	The option 2.7.3 for W Injection be is mishand	s has Ob ie + cha	N/A			PT-OPTI- 919/408		
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	k CVE ID		Patch	1	NCIIPC ID
Component ('Injection')									
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component ('Injection')	22-08-2019	7.5	The option 2.7.3 for W Injection be classes are	ordPressecause se mishano	s has Ob erialized lled.	ject l	N/A		OPT-OPTI- 50919/409
Otrs									
otrs						_			
Information Exposure	21-08-2019	4.3	Ticket Requestion Community 5.0.36 and user logged might unknown session ID I an embedd third parties be then be order to impuser.						OTR- ΓRS- 50919/410
N/A	21-08-2019	4	7.0.x through 7.0.x through 7.0.x through 7.0.36 and An attacker OTRS as an appropriate leverage Of templates in the second results of the second results	as discovered in Open uest System (OTRS) gh 7.0.8, and y Edition 5.0.x through 6.0.x through 6.0.x through is logged into a agent user with the permissions can TRS notification tags in in order to disclose er passwords.			N/A	0'	OTR- FRS- 50919/411
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	scription 8	& CVE ID		Patch		N	CIIPC ID
			CVE ID : C	VE-2019	-13458					
Paloaltonety	works									
twistlock										
N/A	23-08-2019	6	vulnerabil Networks 19.07.358 Twistlock capabilitie to that of interactio componer payload to	Escalation of privilege vulnerability in the Palo Alto Networks Twistlock console 19.07.358 and earlier allows a Twistlock user with Operator capabilities to escalate privileges to that of another user. Active interaction with an affected component is required for the payload to execute on the victim.				/se dvi oal tw m/ det		AL-TWIS- 919/412
pancurses_p	roject									
pancurses										
Use of Externally- Controlled Format String	26-08-2019	6.4	An issue very pancurses for Rust. per have form vulnerabilic CVE ID: C	crate thr rintw and at string ities.	ough 0.2	16.1 ntw	N/A		A-P. PAN 060	
pivotal_softv	ware									
application_	service									
Improper Access Control	19-08-2019	4.1	Pivotal Apin Pivotal versions 2 2.4.x prior 2.5.8, and makes a relocation for a could eave traffic and unencrypt attacker to	https://votal.io ecurity/ e-2019- 11276	/s /cv		IV-APPL- 919/414			
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	6-7	7-8	8	-9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user has over an app. They may also modify the logging level, potentially leading to lost information that would otherwise have been logged. CVE ID: CVE-2019-11276		
raml-modul	e-builder_pro	iect	0.2.5.0.2.20.7.2.2.0		
raml-modul					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	26-08-2019	7.5	Raml-Module-Builder 26.4.0 allows SQL Injection in PostgresClient.update. CVE ID: CVE-2019-15534	N/A	A-RAM- RAML- 060919/415
Rapid7					
nexpose					
Insufficient Session Expiration	21-08-2019	6.8	Rapid7 Nexpose versions 6.5.50 and prior suffer from insufficient session expiration when an administrator performs a security relevant edit on an existing, logged on user. For example, if a user's password is changed by an administrator due to an otherwise unrelated credential leak, that user account's current session is still valid after the password change, potentially allowing the attacker who originally compromised the credential to remain logged in and able to cause further damage. CVE ID: CVE-2019-5638	https://h elp.rapid7 .com/nex pose/en- us/releas e- notes/arc hive/201 9/02/	A-RAP- NEXP- 060919/416
insightapps	ec				l

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	19-08-2019	9.3	The Rapid7 InsightAppSec broker suffers from a DLL injection vulnerability in the 'prunsrv.exe' component of the product. If exploited, a local user of the system (who must already be authenticated to the operating system) can elevate their privileges with this vulnerability to the privilege level of InsightAppSec (usually, SYSTEM). This issue affects version 2019.06.24 and prior versions of the product. CVE ID: CVE-2019-5631	https://h elp.rapid7 .com/insi ghtappsec /release- notes/arc hive/201 9/07/	A-RAP-INSI- 060919/417
riot-os					
riot					
Uncontrolle d Resource Consumptio n	17-08-2019	7.8	RIOT through 2019.07 contains a memory leak in the TCP implementation (gnrc_tcp), allowing an attacker to consume all memory available for network packets and thus effectively stopping all network threads from working. This is related to _receive in sys/net/gnrc/transport_layer/tc p/gnrc_tcp_eventloop.c upon receiving an ACK before a SYN. CVE ID: CVE-2019-15134	N/A	A-RIO-RIOT- 060919/418
Roundcube					
webmail					
Improper Input Validation	19-08-2019	4.3	Roundcube Webmail through 1.3.9 mishandles Punycode xn domain names, leading to homograph attacks. CVE ID: CVE-2019-15237	N/A	A-ROU- WEBM- 060919/419
sailpoint					
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
desktop_pas	sword_reset				
N/A	20-08-2019	6.9	An unauthenticated privilege escalation exists in SailPoint Desktop Password Reset 7.2. A user with local access to only the Windows logon screen can escalate their privileges to NT AUTHORITY\System. An attacker would need local access to the machine for a successful exploit. The attacker must disconnect the computer from the local network / WAN and connect it to an internet facing access point / network. At that point, the attacker can execute the password-reset functionality, which will expose a web browser. Browsing to a site that calls local Windows system functions (e.g., file upload) will expose the local file system. From there an attacker can launch a privileged command shell. CVE ID: CVE-2019-12889	N/A	A-SAI-DESK-060919/420
schine.game	es				
mw-oauth2	client				
Cross-Site Request Forgery (CSRF)	19-08-2019	6.8	In the OAuth2 Client extension before 0.4 for MediaWiki, a CSRF vulnerability exists due to the OAuth2 state parameter not being checked in the callback function. CVE ID: CVE-2019-15150	N/A	A-SCH-MW- O- 060919/421
search-guar	d				
search_guar	d				
Information Exposure	23-08-2019	4	Search Guard versions before 23.1 had an issue that an	N/A	A-SEA-SEAR- 060919/422
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Des	cription 8	k CVE ID		Patch		NCIIPC ID
			administrative bcr of other use internal use	rypt pas ers confi	sword h gured ir	ashes			
			CVE ID : CV	E-2019	-13421				
URL Redirection to Untrusted Site ('Open Redirect')	23-08-2019	5.8	Search Guaversions be before 6.x.y an attacker to a potentiupon Kiban CVE ID : CV	fore 5.6 r-12 had can red ally mal a login.	.8-7 and an issue irect the icious si	e that user te	N/A		A-SEA-SEAR- 060919/423
N/A	23-08-2019	6.5	Search Guaversions be before 6.x.y an authenticould impekibanaserv providing when all of conditions is configure On as auther of Kerberos certificate. user is configured authenticate Basic at the CVE ID: CV	fore 5.6 r-12 had cated Ki rsonate er user v vrong cr the follo a-c are t ed to use enticatio s, JWT, P b) The k igured t e authen Search (to use a ion dom e same ti	8-7 and an issue bana us as when edential wing rue: a) Fe Singlen method is an ase o use H' tication Guard is an SSO hain and me	e that er Sibana Sign- od, one ent rver TTP	N/A		A-SEA-SEAR- 060919/424
Sonatype									
nexus_repos	sitory_manag	er							
Improper Neutralizati on of Input During Web Page	22-08-2019	3.5	In Nexus Rebefore 3.18 privileges C	.0, users	with el	evated I XSS.	N/A]	A-SON- NEXU- 060919/425
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
Generation ('Cross-site Scripting')					
sphinxsearc	h				
sphinx					
Missing Authenticat ion for Critical Function	22-08-2019	5	Sphinx Technologies Sphinx 3.1.1 by default has no authentication and listens on 0.0.0.0, making it exposed to the internet (unless filtered by a firewall or reconfigured to listen to 127.0.0.1 only). CVE ID: CVE-2019-14511	N/A	A-SPH-SPHI- 060919/426
spoon-librar	Ty				•
spoon_librai	ry				
Deserializat ion of Untrusted Data	26-08-2019	7.5	Spoon Library through 2014-02- 06, as used in Fork CMS before 1.4.1 and other products, allows PHP object injection via a cookie containing an object. CVE ID: CVE-2019-15521	N/A	A-SPO-SPOO- 060919/427
status_board	l_project				
status_board	i				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	26-08-2019	4.3	Status Board 1.1.81 has reflected XSS via logic.ts. CVE ID : CVE-2019-15478	N/A	A-STA-STAT- 060919/428
Improper Neutralizati on of Input During Web Page Generation	26-08-2019	4.3	Status Board 1.1.81 has reflected XSS via dashboard.ts. CVE ID: CVE-2019-15479	N/A	A-STA-STAT- 060919/429
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7 137	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site					
Scripting')					
swoole					
swoole					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-08-2019	5	Swoole before 4.2.13 allows directory traversal in swPort_http_static_handler. CVE ID: CVE-2019-15518	N/A	A-SW0- SW00- 060919/430
Telegram					
telegram					
Information Exposure	23-08-2019	5	The Privacy > Phone Number feature in the Telegram app 5.10 for Android and iOS provides an incorrect indication that the access level is Nobody, because attackers can find these numbers via the Group Info feature, e.g., by adding a significant fraction of a region's assigned phone numbers. CVE ID: CVE-2019-15514	N/A	A-TEL-TELE 060919/431
thedaylights	studio				
fuel_cms					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	3.5	FUEL CMS 1.4.4 has XSS in the Create Blocks section of the Admin console. This could lead to cookie stealing and other malicious actions. This vulnerability can be exploited with an authenticated account but can also impact unauthenticated visitors.	N/A	A-THE- FUEL- 060919/432
CV Scoring Scale					

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15228		
Cross-Site Request Forgery (CSRF)	19-08-2019	6.8	FUEL CMS 1.4.4 has CSRF in the blocks/create/ Create Blocks section of the Admin console. This could lead to an attacker tricking the administrator into executing arbitrary code via a specially crafted HTML page. CVE ID: CVE-2019-15229	N/A	A-THE- FUEL- 060919/433
Tibco					
ftl					
N/A	20-08-2019	6.5	The realm configuration component of TIBCO Software Inc.'s TIBCO FTL Community Edition, TIBCO FTL Developer Edition, TIBCO FTL Enterprise Edition contains a vulnerability that theoretically fails to properly enforce access controls. This issue affects TIBCO FTL Community Edition 6.0.0; 6.0.1; 6.1.0, TIBCO FTL Developer Edition 6.0.1; 6.1.0, and TIBCO FTL Enterprise Edition 6.0.0; 6.0.1; 6.1.0. CVE ID: CVE-2019-11209	https://w ww.tibco. com/supp ort/advis ories/201 9/08/tibc o- security- advisory- august- 20-2019- tibco-ftl	A-TIB-FTL- 060919/434
Tiki					
tikiwiki_cms	s/groupware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	22-08-2019	3.5	tiki/tiki-upload_file.php in Tiki 18.4 allows remote attackers to upload JavaScript code that is executed upon visiting a tiki/tiki- download_file.php?display&fileId = URI. CVE ID: CVE-2019-15314	N/A	A-TIK-TIKI- 060919/435
Trendmicro					•

CV Scoring Scale	0-1	1.2	2-3	2.4	4-5	5-6	6.7	70	ο 0	0.10
(CVSS)	0-1	1-2	2-3	3-4	4-3	3-0	6-7	7-0	0-3	9-10

Weakness	Publish Date	cvss	Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
password_m	anager									
Untrusted Search Path	20-08-2019	9.3	A DLL hijadexists in Tr Manager 5. exploited, vattacker to unsigned E service's provery similal CVE-2019-	end Mica 0 in whi would all load an LL into to cocess. To r, yet no 14687.	ro Passw ch, if low an arbitrar che signe his proc t identic	y ed eess is	N/A			RE-PASS- 919/436
Untrusted Search Path	20-08-2019	6.8	A DLL hijadexists in Tr Manager 5. exploited, vattacker to unsigned E service's pr very simila CVE-2019-	end Mica 0 in whi would all load an LL into to cocess. To r, yet no 14684.	ro Passw ch, if low an arbitrar che signe his proc t identic	y ed eess is	N/A			RE-PASS- 919/437
antivirus_se	curity_2019									
N/A	21-08-2019	7.2	A local priv vulnerabili Micro Secu which, if ex an attacker specific pro malicious s	ty exists rity 2019 points of the manifest of the manifest of the existence of the existenc	in Treno 9 (v15.0 would a pulate a ture to l) in llow load a	N/A			RE-ANTI- 919/438
Untrusted Search Path	21-08-2019	6.8	A DLL hijadexists in the Security's 2 of products component Trend Micritool in which allow an attendicious I	e Trend 2019 cons (v15) F t and the ro Ranso ch, if exp	Micro sumer f older Sh standal m Buste loited, v	amily nield one r (1.0)	https://upport.ndmicrom/en-us/hompages/fihical-support.123421	itre fo.c ne/ tec t/1		RE-ANTI- 919/439
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch	1	N	CIIPC ID
			elevated pr	ivileges.			px			
			CVE ID : CV	/E-2019	-14686					
internet_sec	urity_2019							•		
N/A	21-08-2019	7.2	A local priv vulnerabili Micro Secu which, if ex an attacker specific pro malicious s	ty exists rity 2019 ploited, to mani oduct fea ervice.	in Trend 9 (v15.0 would a pulate a ture to l) in llow	N/A			RE-INTE- 919/440
Untrusted Search Path	21-08-2019	6.8	A DLL hijace exists in the Security's 2 of products component Trend Micr tool in which allow an atmalicious I elevated process (CVE ID : CVE ID : C	e Trend 12019 con s (v15) F and the o Ranso ch, if exp tacker to DLL, lead ivileges.	Micro sumer f older Sh standal m Buste loited, v load a ing to	amily ield one r (1.0) vould	https://upport.ndmicrom/en-us/hompages/thnical-support.123421	tre o.c - ne/ tec t/1		RE-INTE- 919/441
maximum_s	ecurity_2019									
N/A	21-08-2019	7.2	A local priv vulnerabili Micro Secu which, if ex an attacker specific pro malicious s	ty exists rity 2019 ploited, to mani oduct fea ervice.	in Treno 9 (v15.0 would a pulate a ture to l) in llow oad a	N/A		A-ΤΊ ΜΑΣ 060	
Untrusted Search Path	21-08-2019	6.8	A DLL hijac exists in the Security's 2 of products component Trend Micr tool in whice	king vul e Trend I 2019 con s (v15) F and the	nerabili Micro sumer f older Sh standal m Buste	ty family ield one r (1.0)	https://upport.ndmicrom/en-us/hompages/thical-	o.c ne/	A-TI MAX 060	
CV Scoring Scale (CVSS)	0-1 1-2	2 2	3-4	4-5	5-6	6-7	7-8	8-	-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to load a malicious DLL, leading to elevated privileges. CVE ID: CVE-2019-14686	support/1 123421.as px	
premium_se	curity_2019				
N/A	21-08-2019	7.2	A local privilege escalation vulnerability exists in Trend Micro Security 2019 (v15.0) in which, if exploited, would allow an attacker to manipulate a specific product feature to load a malicious service. CVE ID: CVE-2019-14685	N/A	A-TRE- PREM- 060919/444
Untrusted Search Path	21-08-2019	6.8	A DLL hijacking vulnerability exists in the Trend Micro Security's 2019 consumer family of products (v15) Folder Shield component and the standalone Trend Micro Ransom Buster (1.0) tool in which, if exploited, would allow an attacker to load a malicious DLL, leading to elevated privileges. CVE ID: CVE-2019-14686	https://es upport.tre ndmicro.c om/en- us/home/ pages/tec hnical- support/1 123421.as px	A-TRE- PREM- 060919/445
ransom_bus	ter				
Untrusted Search Path	21-08-2019	6.8	A DLL hijacking vulnerability exists in the Trend Micro Security's 2019 consumer family of products (v15) Folder Shield component and the standalone Trend Micro Ransom Buster (1.0) tool in which, if exploited, would allow an attacker to load a malicious DLL, leading to elevated privileges. CVE ID: CVE-2019-14686	https://es upport.tre ndmicro.c om/en- us/home/ pages/tec hnical- support/1 123421.as px	A-TRE- RANS- 060919/446
Valvesoftwa	re				

-08-2019	7.2 6.9	Valve Steam Client for Windows through 2019-08-16 allows privilege escalation (to NT AUTHORITY\SYSTEM) because local users can replace the current versions of SteamService.exe and SteamService.dll with older versions that lack the CVE-2019-14743 patch. CVE ID: CVE-2019-15315 Valve Steam Client for Windows through 2019-08-20 has weak folder permissions, leading to privilege escalation (to NT AUTHORITY\SYSTEM) via crafted use of CreateMountPoint.exe and SetOpLock.exe to leverage a TOCTOU race condition. CVE ID: CVE-2019-15316	N/A	A-VAL-STEA 060919/447 A-VAL-STEA 060919/448
		through 2019-08-16 allows privilege escalation (to NT AUTHORITY\SYSTEM) because local users can replace the current versions of SteamService.exe and SteamService.dll with older versions that lack the CVE-2019-14743 patch. CVE ID: CVE-2019-15315 Valve Steam Client for Windows through 2019-08-20 has weak folder permissions, leading to privilege escalation (to NT AUTHORITY\SYSTEM) via crafted use of CreateMountPoint.exe and SetOpLock.exe to leverage a TOCTOU race condition.	,	060919/447
-08-2019	6.9	Valve Steam Client for Windows through 2019-08-20 has weak folder permissions, leading to privilege escalation (to NT AUTHORITY\SYSTEM) via crafted use of CreateMountPoint.exe and SetOpLock.exe to leverage a TOCTOU race condition.	N/A	
<u> </u>				i
-08-2019	6	REDCap before 9.3.0 allows time-based SQL injection in the edit calendar event via the cal_id parameter, such as cal_id=55 and sleep(3) to Calendar/calendar_popup_ajax.p hp. The attacker can obtain a user's login sessionid from the database, and then re-login into REDCap to compromise all data. CVE ID: CVE-2019-14937	https://w ww.evms. edu/resea rch/resou rces_servi ces/redca p/redcap_ change_lo g/	A-VAN- REDC- 060919/449
-08-2019	3.5	REDCap before 9.3.0 allows XSS attacks against non-administrator accounts on the Data Import Tool page via a CSV	https://w ww.evms. edu/resea rch/resou	A-VAN- REDC- 060919/450
			sleep(3) to Calendar/calendar_popup_ajax.p hp. The attacker can obtain a user's login sessionid from the database, and then re-login into REDCap to compromise all data. CVE ID: CVE-2019-14937 REDCap before 9.3.0 allows XSS attacks against non- administrator accounts on the	sleep(3) to Calendar/calendar_popup_ajax.p hp. The attacker can obtain a user's login sessionid from the database, and then re-login into REDCap to compromise all data. CVE ID: CVE-2019-14937 REDCap before 9.3.0 allows XSS attacks against non- administrator accounts on the rch/resou rces_servi ces/redca p/redcap_ change_lo g/ https://w ww.evms.

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Page Generation ('Cross-site Scripting')			data import file. CVE ID: CVE-2019-15127	rces_servi ces/redca p/redcap_ change_lo g/					
webassembl	ly								
binaryen									
NULL Pointer Dereferenc e	28-08-2019	5	An issue was discovered in Binaryen 1.38.32. Two visitors in ir/ExpressionManipulator.cpp can lead to a NULL pointer dereference in wasm::LocalSet::finalize in wasm/wasm.cpp. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by wasm2js. CVE ID: CVE-2019-15759	N/A	A-WEB- BINA- 060919/451				
Webmin				<u>'</u>					
webmin									
Improper Restriction of XML External Entity Reference ('XXE')	26-08-2019	6.8	xmlrpc.cgi in Webmin through 1.930 allows authenticated XXE attacks. By default, only root, admin, and sysadm can access xmlrpc.cgi. CVE ID: CVE-2019-15641	N/A	A-WEB- WEBM- 060919/452				
webp_expre	ss_project								
webp_expre	SS								
Information Exposure	The webp-express plugin before 0.14.11 for WordPress has insufficient protection against arbitrary file reading. CVE ID: CVE-2019-15330		N/A	A-WEB- WEBP- 060919/453					
webtoffee									
import_export_wordpress_users									

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

Weakness	Publish Dat	e C\	VSS		Des	cription 8	k CVE ID		Patch	1	NCIIPC ID
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component ('Injection')	23-08-201	9 6		Imp Wo in t firs colu cre WF er o	& WooCommerce Customers Import Export" plugin 1.3.0 for WordPress allows CSV injection in the user_url, display_name, first_name, and last_name columns in an exported CSV file created by the WF_CustomerImpExpCsv_Export er class. CVE ID: CVE-2019-15092					IN	-WEB- 1PO- 50919/454
Woocomme											
paypal_chec	kout_paym	ent_g	atev						T		
Improper Input Validation	29-08-201	9 5		Wo Pay for Tar par der iter pric	woComm went Ga WordPr mpering cameter monstration on for low ce.	bscr?cm erce Pay ateway p ess allow in an an (such as ted by power than VE-2019	Pal Cheolugin 1. ws Paramount amount urchasin	ckout 6.17 neter (_1), as ig an ended	N/A	P	-W00- AYP- 60919/455
payu_india_j	payment_g	atewa	ıy								
Improper Input Validation	29-08-201	9 5		Wo Pay Wo Tar pur as can inte	/payu/icpcheckout/ in the WooCommerce PayU India Payment Gateway plugin 2.1.1 for WordPress allows Parameter Tampering in the purchaseQuantity=1 parameter, as demonstrated by purchasing an item for lower than the intended price.			N/A	P	-W00- AYU- 60919/456	
G	J C1			CVE ID : CVE-2019-14978							
wp_front_en		rojec	:t								
wp_front_en				The up front and profile plusing			lugis		Α	M/D	
Improper Neutralizati	21-08-201	9 4.	3	The wp-front-end-profile plugin before 0.2.2 for WordPress has				•	N/A		·WP ′P_F-
CV Scoring Scale (CVSS)	0-1	1-2	2	3	3-4	-4 4-5 5-6 6-7				8-9	9-10

Weakness	Publish Date	cvss		Des	cription 8	CVE ID		Patch	ו	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			XSS. CVE I	ID : CV	Æ-2019	-15110			0	60919/457
N/A	21-08-2019	7.5	befor privil	e 0.2.2 lege es	nt-end- _l 2 for Wo calation E-2019	rdPress issue.	has a	N/A	W	-WP /P_F- 60919/458
wpmadeasy										
shortcode_fa	actory									
Improper Input Validation	22-08-2019	7.5	befor Local	e 2.8 f File I	ode-factor for Word nclusion E-2019	lPress h	as	N/A	S	-WPM- HOR- 60919/459
wp-member	s_project									
wp-member	'S									
Cross-Site Request Forgery (CSRF)	27-08-2019	6.8	3.2.8	for W	mbers p ordPres E-2019	s has CS	RF.	N/A	M	-WPWP- I- 60919/460
wp-slimstat										
slimstat_ana	lytics									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	21-08-2019	4.3	4.8.1	The wp-slimstat plugin before 4.8.1 for WordPress has XSS. CVE ID: CVE-2019-15112		N/A		-WPSLIM- 60919/461		
wpsupportp	lus									
wp_support	_plus_respon	sive_tio	cket_sy	stem						
Improper Neutralizati	22-08-2019	4.3			pport-pl m plugi	_		N/A		-WPS- /P_S-
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3	3 3-4 4-5 5-6 6-7				7-8	8-9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
on of Special Elements in Output Used by a Downstrea m Component ('Injection')			for WordPress has HTML injection. CVE ID: CVE-2019-15331						060	919/462
Wso2 api_manage	n									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	16-08-2019	3.5	An issue wa API Manage CARBON-P. There is XS filename to feature of to component CVE ID : CV	er 2.6.0 l ATCH-4. S via a c the file- he event	pefore W 4.0-445 rafted upload simulat	/SO2- 7.	N/A			/SO-API 919/463
xm-online										
Xm^online_2	2common_	utils_aı	nd_endpoin	ts						
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	26-08-2019	7.5	XM^online Endpoints (injection, re Constants.j. DropSchem SchemaCha CVE ID : CV	0.2.1 allo elated to ava, naResolv ingeReso	ows SQL er.java, olver.jav	and a.	N/A		A-XI XM′ 060	
Xymon										
Improper Restriction of Operations within the	27-08-2019	7.5	In Xymon through 4.3.28, a buffer overflow exists in the status-log viewer CGI because of expansion in appfeed.c.			s-log	https://ts.xymocom/arive/201	on. Ich 19-	A-X' XYM 060	
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			CVE ID : CVE-2019-13484	70.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-2019	7.5	In Xymon through 4.3.28, a stack-based buffer overflow vulnerability exists in the history viewer component via a long hostname or service parameter to history.c. CVE ID: CVE-2019-13485	https://lis ts.xymon. com/arch ive/2019- July/0465 70.html	A-XYM- XYMO- 060919/466
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-2019	7.5	In Xymon through 4.3.28, a stack-based buffer overflow exists in the status-log viewer component because of expansion in svcstatus.c. CVE ID: CVE-2019-13486	https://lis ts.xymon. com/arch ive/2019- July/0465 70.html	A-XYM- XYMO- 060919/467
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	27-08-2019	4.3	In Xymon through 4.3.28, an XSS vulnerability exists in the csvinfo CGI script due to insufficient filtering of the db parameter. CVE ID: CVE-2019-13274	https://lis ts.debian. org/debia n-lts- announce /2019/08 /msg0003 2.html	A-XYM- XYMO- 060919/468
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-2019	7.5	In Xymon through 4.3.28, a buffer overflow vulnerability exists in history.c. CVE ID: CVE-2019-13451	https://lis ts.xymon. com/arch ive/2019- July/0465 70.html	A-XYM- XYMO- 060919/469
Improper Restriction of Operations within the	27-08-2019	7.5	In Xymon through 4.3.28, a buffer overflow vulnerability exists in reportlog.c. CVE ID: CVE-2019-13452	https://lis ts.xymon. com/arch ive/2019- July/0465	A-XYM- XYMO- 060919/470
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	cvss	Des	cription 8	k CVE ID		Patch		NCIIPC ID
Bounds of a Memory Buffer							70.html		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-2019	7.5	vulnerability exists in the alert acknowledgment CGI tool because of expansion in acknowledge.c.				https:// ts.xymor com/arc ive/201 July/046 70.html	n. ch 9-	-XYM- YMO- 60919/471
yofla									
360_product	t_rotation								
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	4.3	The 360-pr before 1.4.8 reflected XS CVE ID : CV	3 for Wo SS.	rdPress	_	N/A		-Y0F-360 50919/472
youphptube									
youphptube									
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	20-08-2019	5	plugin/Aud .php in You allows SQL CVE ID : CV	PHPTub Injectio	e throug n.		N/A	Y	-YOU- OUP- 60919/473
Zabbix									
Zabbix									
Information Exposure	17-08-2019	5	Zabbix through 4.4.0alpha1 allows User Enumeration. With login requests, it is possible to			Vith	N/A	Z	-ZAB- ABB- 60919/474
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enumerate application usernames based on the variability of server responses (e.g., the "Login name or password is incorrect" and "No permissions for system access" messages, or just blocking for a number of seconds). This affects both api_jsonrpc.php and index.php. CVE ID: CVE-2019-15132		
Zenoss					
Zenoss					
N/A	21-08-2019	7.2	pyraw in Zenoss 2.5.3 allows local privilege escalation by modifying environment variables to redirect execution before privileges are dropped, aka ZEN-31765. CVE ID: CVE-2019-14257	https://w ww.coalfi re.com/T he- Coalfire- Blog/Aug ust- 2019/Get ting- more- from-a- complianc e-test	A-ZEN- ZENO- 060919/475
Improper Restriction of XML External Entity Reference ('XXE')	21-08-2019	5	The XML-RPC subsystem in Zenoss 2.5.3 allows XXE attacks that lead to unauthenticated information disclosure via port 9988. CVE ID: CVE-2019-14258	https://w ww.coalfi re.com/T he- Coalfire- Blog/Aug ust- 2019/Get ting- more- from-a- complianc e-test	A-ZEN- ZENO- 060919/476

Weakness	Publish Date	CVSS	De	scription 8	& CVE ID		Patch	n l	NCIIPC ID
Zoho									
salesiq									
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	27-08-2019	4.3	The zoho- 1.0.9 for V XSS. CVE ID : 0	s has sto	N/A		ZOH-SALE- 0919/477		
Cross-Site Request Forgery (CSRF)	27-08-2019	6.8	The zoho- 1.0.9 for V	s has CS	N/A		ZOH-SALE- 0919/478		
			Opera	iting Syst	tem				
belwith-kee	ler								
hickory_sma	rt_ethernet_l	oridge_	firmware						
Information Exposure	22-08-2019	5	A cleartex sensitive is vulnerabit Hickory S from Belv Captured Hickory S device connetwork to without un exposed to and passive authentics. This issue Ethernet H077646 appear to informatic CVE ID: C	sent in sent in ernet Britals that fernet Britals the ernet Britals over T broke to MQTT bickory Sodel nurware do ersionin	N/A		BEL-HICK- 0919/479		
Canonical									
ubuntu_linu	x								
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Divide By Zero	17-08-2019	4.3	In GIFLIB before 2019-02-16, a malformed GIF file triggers a divide-by-zero exception in the decoder function DGifSlurp in dgif_lib.c if the height field of the ImageSize data structure is equal to zero. CVE ID: CVE-2019-15133	N/A	O-CAN- UBUN- 060919/480
Cisco					
hyperflex_hx	x220c_edge_n	15_firn	ıware		
N/A	21-08-2019	5.8	A vulnerability in Cisco HyperFlex Software could allow an unauthenticated, remote attacker to perform a man-in-the- middle attack. The vulnerability is due to insufficient key management. An attacker could exploit this vulnerability by obtaining a specific encryption key for the cluster. A successful exploit could allow the attacker to perform a man-in-the-middle attack against other nodes in the cluster. CVE ID: CVE-2019-12621	N/A	O-CIS-HYPE- 060919/481
telepresence	e_codec_c60_f	irmwa	re		•
N/A	21-08-2019	7.2	A vulnerability in Cisco RoomOS Software could allow an authenticated, local attacker to write files to the underlying filesystem with root privileges. The vulnerability is due to insufficient permission restrictions on a specific process. An attacker could exploit this vulnerability by logging in to an affected device with remote support credentials and initiating the specific process on the device	N/A	O-CIS-TELE- 060919/482
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7 152	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and sending crafted data to that process. A successful exploit could allow the attacker to write files to the underlying file system with root privileges. CVE ID: CVE-2019-12622		
hyperflex_h	x220c_af_m5_	firmw	are		
N/A	21-08-2019	5.8	A vulnerability in Cisco HyperFlex Software could allow an unauthenticated, remote attacker to perform a man-in-the- middle attack. The vulnerability is due to insufficient key management. An attacker could exploit this vulnerability by obtaining a specific encryption key for the cluster. A successful exploit could allow the attacker to perform a man-in-the-middle attack against other nodes in the cluster. CVE ID: CVE-2019-12621	N/A	O-CIS-HYPE- 060919/483
hyperflex_h	x220c_m5_fir	mware			
N/A	21-08-2019	5.8	A vulnerability in Cisco HyperFlex Software could allow an unauthenticated, remote attacker to perform a man-in-the- middle attack. The vulnerability is due to insufficient key management. An attacker could exploit this vulnerability by obtaining a specific encryption key for the cluster. A successful exploit could allow the attacker to perform a man-in-the-middle attack against other nodes in the cluster. CVE ID: CVE-2019-12621	N/A	O-CIS-HYPE- 060919/484

Weakness	Publish Date	cvss	[Description 8	& CVE ID		Patch		NC	CIIPC ID
hyperflex_hx	x240c_af_m5_	firmwa	are							
N/A	21-08-2019	5.8	A vulner HyperFl an unaut attacker middle a is due to manager exploit t obtainin key for t exploit o to perfor attack ag cluster. CVE ID:	N/A			S-HYPE- 019/485			
hyperflex_hx	x240c_m5_fir	mware								
N/A	21-08-2019	5.8	A vulner HyperFl an unaut attacker middle a is due to manager exploit t obtainin key for t exploit o to perfor attack ag cluster. CVE ID:	N/A			S-HYPE- 019/486			
telepresence	e_codec_c40_f	irmwa	re							
N/A	21-08-2019	7.2	A vulner Software authenti write file filesyste The vulr	N/A			S-TELE- 019/487			
CV Scoring Scale (CVSS)	0-1 1-2	2 2	2-3 3-4 4-5 5-6 6-7				7-8	8-9	9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient permission restrictions on a specific process. An attacker could exploit this vulnerability by logging in to an affected device with remote support credentials and initiating the specific process on the device and sending crafted data to that process. A successful exploit could allow the attacker to write files to the underlying file system with root privileges. CVE ID: CVE-2019-12622		
telepresence	e_codec_c90_f	irmwa	re		
N/A	21-08-2019	7.2	A vulnerability in Cisco RoomOS Software could allow an authenticated, local attacker to write files to the underlying filesystem with root privileges. The vulnerability is due to insufficient permission restrictions on a specific process. An attacker could exploit this vulnerability by logging in to an affected device with remote support credentials and initiating the specific process on the device and sending crafted data to that process. A successful exploit could allow the attacker to write files to the underlying file system with root privileges. CVE ID: CVE-2019-12622	N/A	O-CIS-TELE- 060919/488
roomos					
N/A	21-08-2019	7.2	A vulnerability in Cisco RoomOS Software could allow an authenticated, local attacker to write files to the underlying filesystem with root privileges.	N/A	O-CIS- ROOM- 060919/489
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to insufficient permission restrictions on a specific process. An attacker could exploit this vulnerability by logging in to an affected device with remote support credentials and initiating the specific process on the device and sending crafted data to that process. A successful exploit could allow the attacker to write files to the underlying file system with root privileges. CVE ID: CVE-2019-12622		
ios_xe					
Cross-Site Request Forgery (CSRF)	21-08-2019	6.8	A vulnerability in the web-based management interface of Cisco IOS XE New Generation Wireless Controller (NGWC) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on an affected device by using a web browser and with the privileges of the user. CVE ID: CVE-2019-12624	N/A	O-CIS-IOS 060919/490
Debian debian_linux	x				
CV Scoring Scale (CVSS)		2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-2019	7.5	In Xymon through 4.3.28, a buffer overflow exists in the status-log viewer CGI because of expansion in appfeed.c. CVE ID: CVE-2019-13484	https://lis ts.xymon. com/arch ive/2019- July/0465 70.html	O-DEB-DEBI- 060919/491
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-2019	7.5	In Xymon through 4.3.28, a stack-based buffer overflow vulnerability exists in the history viewer component via a long hostname or service parameter to history.c. CVE ID: CVE-2019-13485	https://lis ts.xymon. com/arch ive/2019- July/0465 70.html	O-DEB-DEBI- 060919/492
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-2019	7.5	In Xymon through 4.3.28, a stack-based buffer overflow exists in the status-log viewer component because of expansion in svcstatus.c. CVE ID: CVE-2019-13486	https://lis ts.xymon. com/arch ive/2019- July/0465 70.html	O-DEB-DEBI- 060919/493
Deserializat ion of Untrusted Data	20-08-2019	7.5	In Apache Commons Beanutils 1.9.2, a special BeanIntrospector class was added which allows suppressing the ability for an attacker to access the classloader via the class property available on all Java objects. We, however were not using this by default characteristic of the PropertyUtilsBean. CVE ID: CVE-2019-10086	N/A	O-DEB-DEBI- 060919/494
Information Exposure	21-08-2019	4.3	An issue was discovered in Open Ticket Request System (OTRS) Community Edition 5.0.x through 5.0.36 and 6.0.x through 6.0.19. A user logged into OTRS as an agent	N/A	O-DEB-DEBI- 060919/495
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Dat	e C\	/SS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
				sess an o thir be t ord use	sion ID lembedd d partic then be jet to im r.	owingly by sharing ed ticket es. This i potentia persona VE-2019	ng the ling tarticle dentifier denti	nk of with can ed in gent				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	27-08-201	9 4.	3	In X vul CGI filte	Kymon to nerability script of ering of	hrough 4 ty exists lue to in the db p	4.3.28, a in the ca sufficien aramete	n XSS svinfo at er.	https://ts.debia org/del n-lts- announ /2019/ /msg00 2.html	an. bia ice '08	_	EB-DEBI- 919/496
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-201	9 7.	5	ove hist	In Xymon through 4.3.28, a buffer overflow vulnerability exists in history.c. CVE ID: CVE-2019-13451				https://ts.xymc com/ar ive/202 July/04 70.htm	on. ch 19-		EB-DEBI- 919/497
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-08-201	9 7.	5	ove rep	erflow vi ortlog.c	hrough [,] ulnerabi /E-2019	lity exist	ts in	https://ts.xymo com/ar ive/202 July/04 70.htm	on. cch 19-	_	EB-DEBI- 919/498
Improper Restriction of Operations within the Bounds of a Memory	27-08-201	9 7.	5	In Xymon through 4.3.28, a stack-based buffer overflow vulnerability exists in the alert acknowledgment CGI tool because of expansion in acknowledge.c. CVE ID: CVE-2019-13455				lert on in	https://ts.xymocom/arive/202 July/04 70.htm	on. ch 19-		EB-DEBI- 919/499
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		Des	cription 8	k CVE ID		Patch)	N	CIIPC ID
Buffer											
N/A	21-08-2019	4	Tic 7.0 Cor 5.0 An OT app leve	ket Request through the second	as discovered as	em (OT and 5.0.x the ough 6.0 logged is ser with esions cafication to disclerords.	RS) arough 0.19. nto an tags in	N/A			EB-DEBI- 919/500
Use After Free	20-08-2019	7.2	In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, was incorrectly backported to the earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that was intended to be fixed by backporting. Specifically, by adding to a write queue between disconnection and reconnection, a local attacker can trigger multiple use-after-free conditions. This can result in a kernel crash, or potentially in privilege escalation. NOTE: this affects (for example) Linux distributions that use 4.9.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.14.139.				N/A			EB-DEBI- 919/501	
Improper Restriction of Operations	21-08-2019	6.8	An issue was discovered in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The faad_resetbits function in								
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	cvss		Desc	ription 8	CVE ID		Patch	1	N	ICIIPC ID
within the Bounds of a Memory Buffer			libfaad/bits.c is affected by a buffer overflow vulnerability. The number of bits to be read is determined by ld->buffer_size - words*4, cast to uint32. If ld- >buffer_size - words*4 is negative, a buffer overflow is later performed via getdword_n(&ld->start[words], ld->bytes_left). CVE ID: CVE-2019-15296								
Dlink											
dir-823g_fir	mware										
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	23-08-2019	9	An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the Type field to SetWanSettings, a related issue to CVE-2019-13482. CVE ID: CVE-2019-15526				N/A		_	LI-DIR 919/503	
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	23-08-2019	9	An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the MaxIdTime field to SetWanSettings. CVE ID: CVE-2019-15527				N/A			LI-DIR 1919/504	
Improper Neutralizati on of Special Elements used in a Command ('Command	23-08-2019	9	Link D firmwa comma (explo via she	An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the Interface field to							LI-DIR 919/505
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	cvss	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
Injection')			SetStaticRo CVE ID : CV		Ü					
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	23-08-2019	9	An issue was Link DIR-8. firmware V command i (exploitable via shell me Username fice CVE ID : CVE	23G devi 1.0.2B0! njection e with A etachara field to L	ices with 5. There in HNA authentic cters in cogin.	is a P1 ation) the	N/A		_	LI-DIR 919/506
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	23-08-2019	9	An issue wa Link DIR-82 firmware V command i (exploitable via shell me LoginPassv CVE ID : CV	23G devi 1.0.2B0! njection e with A etachara vord fiel	ices with There in HNA uthentic cters in d to Log	is a P1 ation) the in.	N/A		_	LI-DIR 919/507
galliumos										
galliumos										
N/A	22-08-2019	5	In Gallium(CONFIG_SE disabled by ptrace.conf/proc/sys/cope to 1, vrisk because that a protespresent wheeld continued in the continued continued in	curity at /etc/s tries to kernel/y which mi e of the ection m en actua	ysctl.d/i set yama/pt ght incr appeara echanisi	race_s ease nce n is not.	N/A			AL-GALL- 919/508
getvera	MM MATONO									
vera_edge_fi Improper	imware		cgi-bin/cm	h/wehca	ım sh in	Vera				
Neutralizati on of Special	23-08-2019	9.3	Edge Home allows rem users to exc	Control ote unau	ler 1.7.4 ithentica	452 ated	N/A		O-GI VER 0609	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9	9-10

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
Elements used in an OS Command ('OS Command Injection')			inje par bin	commands viaoutput argument injection in the username parameter to /cgi-bin/cmh/webcam.sh. CVE ID: CVE-2019-15498							
nest_cam_iq	_indoor_firm	ware									
Out-of- bounds Read	20-08-2019	5	dis the fun Ind spe car res dis pad vul	exploita closure versectionality cloor versectally crucially crucially crucially crucially crucially crucially crucial cause a closure. ckets to the characteristic contraction of the crucial	vulnerable vulnerable voluments of Nestion 462 afted we informate an attack vilger to the voluments of the voluments of the voluments of Nestinger to the Nestinger to	Pairing of Cam IC of Cam I	sts in Q set of kets read,	N/A	1	0-G0 NES	
Improper Authenticat ion	20-08-2019	6.8	dis the fun Ind spe car res and cor spe trig	exploitaclosure versionality crucially crucial	vulnerate PASE party of the sion 462 afted we preater ially full attacked afted party vulnerate vulnerate party full vulnerate party vulnerate party full vulnerate party full vulnerate party full party	oility exi iring Nest Ca 20002. A eave pace niring co Weave device can ser ckets to bility.	m IQ set of ekets de, access	N/A	1	0-G0 NES'	
Improper Access Control	20-08-2019	7.8	An exploitable denial-of-service vulnerability exists in the Weave error reporting functionality of the Nest Cam IQ Indoor, version 4620002. A specially crafted								
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	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
			weave pack arbitrary V Session to denial of se send a spec trigger this CVE ID : CV	Veave Ex close, res ervice. An cially cra s vulnera	change sulting in attacke fted pac bility.	n a er can				
Integer Overflow or Wraparoun d	20-08-2019	7.8	An exploita vulnerabili certificate Nest Cam I version 46 crafted we an integer of-bounds memory to denial of se send a spectrigger. CVE ID:	ty exists loading f Q Indoor 20002. A ave pack overflow read on to occur, re ervice. An	in the Wunctional cameral special et can can and an unmapp esulting attacked fred pac	Veave ality of ly ause out- ed in a	N/A		O-G NES 060	
Integer Overflow or Wraparoun d	20-08-2019	5	An exploitable information disclosure vulnerability exists in the Weave MessageLayer parsing of Openweave-core version 4.0.2 and Nest Cam IQ Indoor version 4620002. A specially crafted weave packet can cause an integer overflow to occur, resulting in PacketBuffer data reuse. An attacker can send a packet to trigger this vulnerability. CVE ID: CVE-2019-5040				N/A		O-G NES 060	
android										
N/A	20-08-2019	7.2	In ACELP_4t64_fx of c4t64fx.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no				https:// urce.an oid.com ecurity ulletin/	dr 1/s /b	0-G AND 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-132647222. CVE ID: CVE-2019-2128	19-08-01	
Out-of- bounds Read	20-08-2019	4.3	In extract3GPPGlobalDescriptions of TextDescriptions.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-124781927.	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	O-GOO- ANDR- 060919/516
Incorrect Type Conversion or Cast	20-08-2019	10	In CompilationJob::FinalizeJob of compiler.cc, there is a possible remote code execution due to type confusion. This could lead to escalation of privilege from a malicious proxy configuration with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-132073833. CVE ID: CVE-2019-2130	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	0-G00- ANDR- 060919/517

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	20-08-2019	9.3	An application with overlay permission can display overlays on top of settings UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119115683.	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	0-G00- ANDR- 060919/518
N/A	20-08-2019	9.3	It is possible to overlay the VPN dialog by a malicious application. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130568701.	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	0-G00- ANDR- 060919/519
Out-of- bounds Write	20-08-2019	9.3	In Mfc_Transceive of phNxpExtns_MifareStd.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-132082342. CVE ID: CVE-2019-2133	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	0-G00- ANDR- 060919/520

Weakness	Publish Date	cvss	Des	cription 8	CVE ID		Patch	ו	N	CIIPC ID
Integer Overflow or Wraparoun d	20-08-2019	9.3	In phFriNfo phNxpExtn is a possibl due to an in could lead privilege w execution p interaction exploitation Versions: A 7.1.1 Andro Android-8. ID: A-1320	e out of lateger over to local exith no according to the control of the control o	Std.cpp, counds verflow. escalatio ditional s needec ed for ct: Andr 7.0 Andr Android	there write This n of d. User oid. roid- d-8.0	https:// urce.an oid.com ecurity ulletin/ 19-08-0	dr n/s /b /20	0-G AND 060	
Out-of- bounds Read	20-08-2019	7.1	In Mfc_TraphNxpExtrais a possible due to a min This could information additional meeded. Us needed for Android-7. Android-8. Android-9. 125900276 CVE ID: CVE	e out of lassing book lead to look lead to l	Std.cpp, counds a unds cho ocal ure with n privile ction. Pro Android oid-7.1.2 d-8.1 ID: A-	read eck. i no ges oduct: -7.0	https:// urce.an oid.com ecurity ulletin/ 19-08-0	dr n/s /b /20	0-G AND 060	
Out-of- bounds Read	20-08-2019	4.9	In Status::r Status.cpp, of bounds in input valid to local info with no add privileges in interaction exploitation Versions: A	le out oper lead ure n r	https://urce.an oid.com ecurity ulletin/ 19-08-0	dr n/s /b /20	0-G ANE 060			
CV Scoring Scale	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-	.9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Android-8.1 Android-9. Android ID: A-132650049. CVE ID: CVE-2019-2136		
Improper Input Validation	20-08-2019	4.9	In the endCall() function of TelecomManager.java, there is a possible Denial of Service due to a missing permission check. This could lead to local denial of access to Emergency Services with User execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-132438333. CVE ID: CVE-2019-2137	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	O-GOO- ANDR- 060919/524
N/A	20-08-2019	7.2	In OatFileAssistant::GenerateOatFile of oat_file_assistant.cc, there is a possible file corruption issue due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android- 7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130821293. CVE ID: CVE-2019-2120	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	0-G00- ANDR- 060919/525
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race	20-08-2019	6.9	In ActivityManagerService.attachAp plication of ActivityManagerService, there is a possible race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://so urce.andr oid.com/s ecurity/b ulletin/20 19-08-01	0-G00- ANDR- 060919/526

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android ID: A- 127605586. CVE ID: CVE-2019-2122 In ChangeDefaultDialerDialog.java, there is a possible escalation of privilege due to an overlay attack. This could lead to local escalation of privilege, granting privileges to a local app without the user's informed consent, with no additional privileges needed. N/A unlettn/20 19-08-01 19-08-01 19-08-01 19-08-01 19-08-01 0-08-01 19-08-01 19-08-01	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A 20-08-2019 8. DockTaskController.lockKeyguar dlfNeeded of the LockTaskController.java, there was a difference in the handling of the default case between the WindowManager and the Settings. This could lead to a local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android-Y.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android-10. Android-9. Android-10. Android-9. Android-10. Android-9. Android-10. Android-9. Android-10. Android-9. Android-10. Android-	Condition')			Versions: Android-9. Android ID: A-131105245.		
N/A 20-08-2019 4.4 20-08-2019 Android-8.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android-1D: A-132275252. CVE ID : CVE ID : CVE-2019-2125	N/A	20-08-2019	6.9	LockTaskController.lockKeyguar dIfNeeded of the LockTaskController.java, there was a difference in the handling of the default case between the WindowManager and the Settings. This could lead to a local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-127605586.	urce.andr oid.com/s ecurity/b ulletin/20	
Double 20-08-2019 9.3 In ParseContentEncodingEntry of https://so 0-G00-	N/A	20-08-2019	4.4	ChangeDefaultDialerDialog.java, there is a possible escalation of privilege due to an overlay attack. This could lead to local escalation of privilege, granting privileges to a local app without the user's informed consent, with no additional privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-132275252.	urce.andr oid.com/s ecurity/b ulletin/20	
	Double	20-08-2019	9.3	In ParseContentEncodingEntry of	https://so	0-G00-

(CVSS)

Weakness	Publish Date	CVSS	Des	Patch	١	N	CIIPC ID			
Free			mkvparser double free of a freed p to remote additional needed. Us needed for Android. V Android-7 Android-8 Android-9 12770236	a missing cution was priviled action. Proceedings of the contraction of the contraction of the contraction. The contraction of	urce.an oid.com ecurity, ulletin/ 19-08-0	n/s /b /20	AND 060	OR- 919/529		
Use After Free	20-08-2019	7.2	In AudioInpuctive of AudioInpucis possible due to a use lead to local privilege we execution privilege we exploitation Versions: A 7.1.1 Andr Android-8. ID: A-1248	https:// urce.an oid.com ecurity/ ulletin/ 19-08-0	dr n/s /b '20	O-G- ANE 060				
Intel										
compute_car	rd_firmware									
Improper Input Validation	19-08-2019	4.6	Insufficien system firm may allow potentially privilege, conformation access. CVE ID: C	nware fo a privile enable e lenial of n disclos	r Intel(I ged user escalatio service a ure via	https://www.inte om/cornt/www us/en/s urity- center/ visory/	el.c nte w/ sec	O-IN COM 060		
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	6-7	7-8	8	-9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
				el-sa- 00272.ht ml							
compute_sti	ick_firmware										
Improper Input Validation	19-08-2019	4.6	Insufficient session validation in system firmware for Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access. CVE ID: CVE-2019-11140	https://w ww.intel.c om/conte nt/www/ us/en/sec urity- center/ad visory/int el-sa- 00272.ht ml	O-INT- COMP- 060919/532						
nuc_kit_firm	nuc_kit_firmware										
Improper Input Validation	19-08-2019	4.6	Insufficient session validation in system firmware for Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access. CVE ID: CVE-2019-11140	https://w ww.intel.c om/conte nt/www/ us/en/sec urity- center/ad visory/int el-sa- 00272.ht ml	O-INT-NUC 060919/533						
Lenovo											
20ng_firmw	are										
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20NG- 060919/534						
CV Scoring Scale (CVSS)	e 0-1 1-7	2 2	3-4 4-5 5-6 6-7	7-8	9-10						

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch	1	NCIIPC ID
20nn_firmw	are		<u> </u>						
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171						0-LEN- 20NN- 060919/535
20nq_firmw	are								
N/A	19-08-2019	7.2	various BIO ThinkPad s allow a use privileges o ability to u						0-LEN- 20NQ- 060919/536
20nr_firmwa	are								
N/A	19-08-2019	7.2	various BIO ThinkPad s allow a use privileges of ability to up Controller of firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					0-LEN- 20NR- 060919/537
20ns_firmwa	are								
N/A	19-08-2019	7.2	A vulneraby various BIC ThinkPad so allow a use privileges cability to up Controller	ons of old that could dministral cal acces e Embed	N/A		0-LEN-20NS 060919/538		
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3 3-4	-				8-9	9 9-10

Weakness	Publish Dat	e CVSS		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID							
			firr	nware.														
			CV I	E ID : CV	/E-2019	-6171												
20nt_firmwa	are																	
N/A	19-08-201	9 7.2	var Thi allo pri abi Con firr	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171				ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.				various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.			N/A		0-L 20N 060	
20nu_firmw	are																	
N/A	19-08-201	9 7.2	var Thi allo pri abi Con firr	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171				N/A		O-L 20N 060								
230x_firmw	are																	
N/A	19-08-201	9 7.2	var Thi allo pri abi Con firr	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171			rious BIOS versions of older linkPad systems that could ow a user with administrative livileges or physical access the lility to update the Embedded introller with unsigned mware.		various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.		N/A			EN-230X- 919/541				
232x_firmw	are																	
N/A	19-08-201	9 7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative		various BIOS versions of older ThinkPad systems that could		various BIOS versions of older ThinkPad systems that could			various BIOS versions of older ThinkPad systems that could		der ld	N/A			EN-232X- 919/542		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4 4-5 5-6 6-7				7-8	8	-9	9-10							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges or physical access the ability to update the Embedded Controller with unsigned firmware.		
			CVE ID: CVE-2019-6171		
233x_firmw	are				
N/A	19-08-2019	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.		N/A	O-LEN-233X- 060919/543
			CVE ID : CVE-2019-6171		
234x_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-234X- 060919/544
235x_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-235X- 060919/545
239x_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in	N/A	O-LEN-239X-
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7 173	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch	1	N	CIIPC ID
			various BIC ThinkPad s allow a use privileges c ability to up Controller s firmware. CVE ID : CV	ystems to with according to the contract of th	hat coul lministr al acces e Embed igned	d ative s the			060	919/546
242x_firmwa	are									
N/A	19-08-2019	7.2	various BIC ThinkPad s allow a use privileges of ability to up Controller of firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171						EN-242X- 919/547
243x_firmwa	are									
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171				N/A			EN-243X- 919/548
244x_firmwa	are									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller firmware.	N/A			EN-244X- 919/549			
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-	9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
246x_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-246X- 060919/550
247x_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-247X- 060919/551
248x_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-248X- 060919/552
30eh_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned	N/A	O-LEN- 30EH- 060919/553
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware.		
			CVE ID: CVE-2019-6171		
336x_firmw	are				
N/A	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.		N/A	O-LEN-336X- 060919/554	
			CVE ID: CVE-2019-6171		
337x_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-337X- 060919/555
343x_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-343X- 060919/556
344x_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative	N/A	0-LEN-344X- 060919/557
CV Scoring Scale (CVSS)	e 0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Dat	CVS	6	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID									
			abi	vileges of lity to up ntroller nware.	pdate th	e Embec														
			cv	E ID : CV	/E-2019	-6171														
34xx_firmwa	are																			
N/A	19-08-201	7.2	vai Th allo pri abi Co firi	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171				arious BIOS versions of older thinkPad systems that could llow a user with administrative rivileges or physical access the bility to update the Embedded ontroller with unsigned rmware.				N/A			EN-34XX- 919/558					
3xxx_firmwa	are																			
N/A	19-08-201		vai Th allo pri abi Co firr	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171				various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.			N/A			EN-3XXX- 919/559						
home_media	_network_	nard_d	rive_f	irmwar	e															
Information Exposure	19-08-201	9 4.3	vull Ler allo der thr Per do or un con	An information leakage vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents. CVE ID: CVE-2019-6178				An information leakage vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents.				alnerability in Iomega and enovoEMC NAS products could low disclosure of some device etails such as Share names arough the device API when ersonal Cloud is enabled. This pes not allow read, write, delete, any other access to the inderlying file systems and their ontents.			vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents.		N/A		O-L. HON 060	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	2-3 3-4 4-5 5-6 6-7			6-7	7-8	8	-9	9-10									

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
ix12-300r_fi	rmware				
Information Exposure	19-08-2019	4.3	An information leakage vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents. CVE ID: CVE-2019-6178	N/A	O-LEN-IX12- 060919/561
px12-350r_f	irmware				
Information Exposure	19-08-2019	4.3	An information leakage vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents. CVE ID: CVE-2019-6178	N/A	O-LEN-PX12- 060919/562
storecenter_	ix2-200_firm	ware			
Information Exposure	19-08-2019	4.3	An information leakage vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents.	N/A	O-LEN- STOR- 060919/563

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Des	cription 8	CVE ID		Patch	1	N	CIIPC ID	
			CVE	ID : CV	E-2019	-6178						
storecenter_	ix4-200d_fir	mware										
Information Exposure	19-08-2019	4.3	vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents. CVE ID: CVE-2019-6178				LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents. CVE ID: CVE-2019-6178					
storecenter_	ix4-200rl_fir	mware	•									
Information Exposure	19-08-2019	4.3	vulne Leno allow detai throu Perso does or an unde	An information leakage vulnerability in Iomega and LenovoEMC NAS products could allow disclosure of some device details such as Share names through the device API when Personal Cloud is enabled. This does not allow read, write, delete, or any other access to the underlying file systems and their contents.						0-Ll STO 060		
bladecenter	hs22_firmwa	are										
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web					N/A		0-Ll BLA 060		
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4 4-5 5-6 6-7				6-7	7-8 8		9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159		
bladecenter	_hs22v_firmw	are			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A	O-LEN- BLAD- 060919/567
bladecenter	 _hx5_firmwar	·e			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records	N/A	O-LEN- BLAD- 060919/568

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected.		
cyctom v24	00_m3_firmw	aro	CVE ID : CVE-2019-6159		
<i>y</i> –			A stored cross-site scripting		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	(XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A	O-LEN-SYST- 060919/569
system_x35	00_m2_firmw	are			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code	N/A	O-LEN-SYST- 060919/570

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159		
system_x350	00_m3_firmw	are			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A	0-LEN-SYST- 060919/571
system x35	50_m3_firmw	are	CVE ID . CVE-2017-0137		
system_x55	70_III3_III IIIW	ui C	A stored cross-site scripting		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	ralizati Input g Web 19-08-2019 4.3 v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be		N/A	O-LEN-SYST- 060919/572	

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
system x350	50_m2_firmw	are	not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159		
			A stored cross-site scripting (XSS) vulnerability exists in		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A	O-LEN-SYST- 060919/573
system_x363	30_m3_firmw	are			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be		N/A	O-LEN-SYST- 060919/574	

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	N	CIIPC ID
			later IMM2 (IMM v2) is not			
			affected.			
			CVE ID : CVE-2019-6159			
system_x365	50_m3_firmwa	are			·	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A		EN-SYST 919/575
system x36°	90_x5_firmwa	re	CVE ID . CVE-2019-0139			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not	N/A		EN-SYST 919/576
CV Scoring Scale			1000 1111112 (111111 VZ) 13 1100			

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NO	CIIPC ID
			affected.			
			CVE ID : CVE-2019-6159			
system_x385	50_x5_firmwa	re			·	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A	_	:N-SYST- 919/577
system_x395	50_x5_firmwa	re				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected.	N/A		:N-SYST- 919/578
CV Scoring Scale (CVSS)	0-1 1-2	2 2	2-3 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-2019-6159		
system_x_ida	ataplex_dx36	0_m2_f	firmware		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A	O-LEN-SYST- 060919/579
system_x_ida	ataplex_dx36	0_m3_f	irmware		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	19-08-2019	4.3	A stored cross-site scripting (XSS) vulnerability exists in various firmware versions of the legacy IBM System x IMM (IMM v1) embedded Baseboard Management Controller (BMC). This vulnerability could allow an unauthenticated user to cause JavaScript code to be stored in the IMM log which may then be executed in the user's web browser when IMM log records containing the JavaScript code are viewed. The JavaScript code is not executed on IMM itself. The later IMM2 (IMM v2) is not affected. CVE ID: CVE-2019-6159	N/A	O-LEN-SYST- 060919/580
CV Scoring Scale					
(CVSS)	0-1 1-3	2 2	186	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
yoga_700-11	lisk_firmware	9				
Untrusted Search Path	19-08-2019	6.8	A DLL search path vulnerability was reported in PaperDisplay Hotkey Service version 1.2.0.8 that could allow privilege escalation. Lenovo has ended support for PaperDisplay Hotkey software as the Night light feature introduced in Windows 10 Build 1703 provides similar features. CVE ID: CVE-2019-6165	N/A	O-LEN- YOGA- 060919/581	
yoga_700-14	lisk_firmware	9				
Untrusted Search Path	19-08-2019	6.8	A DLL search path vulnerability was reported in PaperDisplay Hotkey Service version 1.2.0.8 that could allow privilege escalation. Lenovo has ended support for PaperDisplay Hotkey software as the Night light feature introduced in Windows 10 Build 1703 provides similar features. CVE ID: CVE-2019-6165	N/A	O-LEN- YOGA- 060919/582	
20a7_firmwa	are					
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	ions of older that could administrative ical access the he Embedded asigned		
20a8_firmware						
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could	N/A	O-LEN-20A8- 060919/584	
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171		
20a9_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20A9- 060919/585
20aa_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	0-LEN- 20AA- 060919/586
20ab_firmw	are			1	
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20AB- 060919/587
20ac_firmw	are		1	1	

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Des	cription 8	CVE ID		Patch	1	NCIIPC ID
N/A	19-08-2019	7.2	A vulneraby various BIO ThinkPad sallow a use privileges of ability to u Controller firmware.	OS version ystems to r with action physicon pdate the with uns	ns of ole hat cou lministr al acces e Embed igned	der ld ative s the	N/A	LEN-20AC- 0919/588	
20aj_firmwa	ire								
N/A	19-08-2019	7.2	A vulneraby various BIO ThinkPad so allow a use privileges of ability to u Controller firmware.	ns of ole hat coul dministral al acces e Embed igned	N/A		LEN-20AJ- 0919/589		
20ak_firmwa	are								
N/A	19-08-2019	7.2	various BIO ThinkPad s allow a use privileges of ability to u Controller firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.				20	LEN- AK- 0919/590
2001 5			CVE ID : CV	/E-2019	-6171				
20al_firmwa	re		Λ11	:1:4	More a -1	d :			
N/A	19-08-2019	7.2	A vulnerab various BIO ThinkPad s allow a use privileges of ability to u Controller firmware.	ons of old that could dministral al acces e Embed	N/A		O-LEN-20AL- 060919/591		
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID	
			CVE	ID : CV	E-2019	-6171						
20am_firmw	vare											
N/A	19-08-2019	7.2	varion Thir allow prive abilic Contractions	ous BIC nkPad s w a use rileges o ity to up troller v nware.	lity was S versic ystems t r with ac r physic odate the with uns	ns of old that count dministral cal acces e Embed signed	der ld rative s the	N/A		O-LEN- 20AM- 060919/592		
20an_firmw	are											
N/A	19-08-2019	7.2	varion Thir allow prive abilic Contractions	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171						O-LEN- 20AN- 060919/593		
20aq_firmw	are											
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					N/A		O-LI 20A 060		
20ar_firmwa	are											
N/A	19-08-2019	7.2	varion Thir allow priv	ous BIC nkPad s w a use rileges o	reporte ons of ol- chat coul dministr cal acces e Embec	N/A		O-LEN- 20AR- 060919/595				
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9	9-10	

Weakness	Publish Date	cvss	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
			Controller of firmware. CVE ID : CV							
20aw_firmw	are									
N/A	19-08-2019	7.2	various BIC ThinkPad s allow a use privileges of ability to up Controller of firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					0-Ll 20A 060	
20b0_firmw	are									
N/A	19-08-2019	7.2	various BIC ThinkPad s allow a use privileges c ability to up						O-LEN-20B0- 060919/597	
20b3_firmw	are									
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171				N/A		O-LEN-20B3- 060919/598	
20b6_firmw	are									
N/A	19-08-2019	7.2	A vulnerabi various BIC ThinkPad s	der	N/A		O-LEN-20B6- 060919/599			
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	4-5	5-6	6-7	7-8	8-	9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171		
20b7_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20B7- 060919/600
20be_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20BE- 060919/601
20bf_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20BF- 060919/602
20bg_firmw	are		1	1	

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch		N	CIIPC ID
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	ns of ole hat cou dministr al acces e Embed igned	N/A		0-Ll 20B 060			
20bl_firmwa	are									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	N/A			EN-20BL- 919/604			
20bm_firmw	vare									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	ns of olo hat cou dministr al acces e Embed igned	N/A		0-Ll 20B 060			
20bu_firmw	are		3.212.01		J _ / _					
2004_III III W			A vulnerab	ility was	reporte	ed in				
N/A	19-08-2019	7.2	various BIC ThinkPad s allow a use privileges of ability to up Controller of firmware.	OS version ystems to with a contract the physical physica	ons of old that could dministral cal acces e Embed	der ld rative s the	N/A		0-Ll 20B 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-	-9	9-10

Weakness	Publish Date	CVSS	De	scription &	& CVE ID		Patch	1	NCIIPC ID
			CVE ID : (VE-2019	-6171				
20bv_firmw	are								
N/A	19-08-2019	7.2	A vulneral various B ThinkPad allow a use privileges ability to Controlled firmware.	OS versions to systems	ons of old chat count dministrated access e Embed signed	N/A	20	-LEN-)BV- 50919/607	
20bw_firmw	are								
N/A	19-08-2019	7.2	A vulnera various B ThinkPad allow a us privileges ability to Controlle firmware.	ons of old chat count dministrated access e Embed signed	N/A	20	-LEN-)BW- 50919/608		
20bx_firmw	are								
N/A	19-08-2019	7.2	various B ThinkPad allow a us privileges ability to Controlles firmware	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					-LEN-20BX- 50919/609
20d9_firmw	are								
N/A	19-08-2019	7.2	A vulnera various B ThinkPad allow a us privileges ability to	OS version systems to the control of	ons of old that could dministrated acces	der ld rative s the	N/A	20	-LEN-)D9- 50919/610
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	scription 8	& CVE ID		Patch	1	NCIIPC ID
			Controller firmware. CVE ID : C						
20da_firmw	are								
N/A	19-08-2019	7.2	A vulneral various BI ThinkPad allow a us privileges ability to u Controller firmware.	ons of old that could dministrated acces to Embed signed	N/A		O-LEN- 20DA- 060919/611		
20dc_firmwa	are								
N/A	19-08-2019	7.2	A vulneral various BI ThinkPad allow a us privileges ability to u Controller firmware.	ons of old that could dministral cal acces e Embed signed	N/A		O-LEN- 20DC- 060919/612		
20dd_firmw	are								
N/A	19-08-2019	7.2	various BI ThinkPad allow a us privileges ability to u						O-LEN- 20DD- 060919/613
20de_firmw	are								
N/A	19-08-2019	7.2	A vulneral various BI ThinkPad	ns of old	der	N/A		O-LEN- 20DE- 060919/614	
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171		
20df_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20DF- 060919/615
20dg_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20DG- 060919/616
20dh_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20DH- 060919/617
20dj_firmwa	are				

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch		N	CIIPC ID
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad s allow a use privileges of ability to up Controller of firmware. CVE ID: CV	ns of ole hat cou dministral al acces e Embed igned	N/A			EN-20DJ- 919/618		
20dq_firmw	are									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	ns of ole hat cou lministral al acces e Embed igned	N/A		0-L 20D 060			
20dr_firmwa	are									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware.	ns of ole hat cou dministr al acces e Embed igned	N/A		0-Li 20D 060			
20ds_firmwa	are		GVE ID . GV	2017	01/1					
2005_III III W			A vulnerab	ility was	reporte	ed in				
N/A	19-08-2019	7.2	various BIC ThinkPad s allow a use privileges c ability to up Controller s firmware.	ons of old that could dministral al acces e Embed	der ld rative s the	N/A			EN-20DS- 919/621	
CV Scoring Scale (CVSS)	0-1 1-2	2 2	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	D	escription &	& CVE ID		Patch	1	NCIIPC ID
			CVE ID:	CVE-2019	-6171				
20dt_firmwa	are								
N/A	19-08-2019	7.2	various E ThinkPad allow a u privilege ability to Controlle firmware	bility was IOS version I systems to ser with a ser or physion update the r with uns CVE-2019	ons of old chat could dministrated access e Embed signed	N/A	2	0-LEN- 0DT- 060919/622	
20e0_firmw	are								
N/A	19-08-2019	7.2	various E ThinkPad allow a u privilege ability to Controlle firmware	Ibility was IOS version I systems to ser with a sor physion update the r with uns c. CVE-2019	ons of old chat could dministrated acces e Embed signed	der ld rative s the	N/A	_	0-LEN-20E0- 060919/623
20ef_firmwa	ire								
N/A	19-08-2019	7.2	A vulnera various E ThinkPac allow a u privilege ability to Controlle firmware CVE ID:	ons of old chat could dministrated access e Embed signed	N/A		0-LEN-20EF- 060919/624		
20eg_firmwa	are								
N/A	19-08-2019	7.2	various E ThinkPac allow a u privilege	Ibility was IOS version I systems to ser with a sor physion update th	ons of old that could dministrated acces	der ld rative s the	N/A		0-LEN-20EG- 060919/625
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
			firn	ıware.	with uns E-2019						
20et_firmwa	ire										
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					N/A		_	EN-20ET- 919/626
20eu_firmwa	are										
N/A	19-08-2019	7.2	vari Thi allo priv abil Con firn	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171						O-Ll 20E 060	
20ev_firmwa	are										
N/A	19-08-2019	7.2	vari Thi allo priv abil Con firm	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. EVE ID: CVE-2019-6171				N/A		_	EN-20EV- 919/628
20ew_firmw	are										
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could					N/A		O-LEN- 20EW- 060919/62	
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
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171		
20ex_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20EX- 060919/630
20ey_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20EY- 060919/631
20f1_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20F1- 060919/632
20f2_firmwa	are				

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Des	cription 8	& CVE ID		Patch		NCIIPC ID
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges coability to up Controller of firmware. CVE ID: CV	OS version ystems to r with accomplying or physicon podate the with uns	ons of old chat cou dministral cal acces e Embed signed	N/A		LEN-20F2- 0919/633	
20f5_firmwa	are								
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	ons of old hat cound dministral cal acces e Embed signed	N/A		LEN-20F5- 0919/634		
20f6_firmwa	are								
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware.	ns of ol hat cou dministr al acces e Embed igned	N/A		LEN-20F6- 0919/635		
20fm_firmw	are								
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad s allow a use privileges of ability to up Controller of firmware.	ons of ole that cou dministral cal acces e Embed	N/A	20	LEN- FM- 0919/636		
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Desc	cription 8	CVE ID		Patch	1	NC	IIPC ID
			CVE I	D : CV	E-2019	-6171					
20fn_firmwa	are										
N/A	19-08-2019	7.2	varion Think allow privil ability Contr	us BIC	lity was S versic ystems t r with ac r physic odate the with uns	ns of old hat could dministral cal acces e Embed igned	N/A]	0-LE 20FN 0609		
20fu_firmwa	are										
N/A	19-08-2019	7.2	varion Think allow privil ability Contr	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171						_	N-20FU- 19/638
20fv_firmwa	ire										
N/A	19-08-2019	7.2	varion Think allow privil ability Contr firmw	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171							N-20FV- 19/639
20fw_firmw	are										
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded					N/A	:	0-LE 20FW 0609	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9)	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned		
			firmware.		
			CVE ID : CVE-2019-6171		
20fx_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20FX- 060919/641
20g4_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.	N/A	O-LEN-20G4- 060919/642
			CVE ID : CVE-2019-6171		
20g5_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.	N/A	O-LEN-20G5- 060919/643
22.2.5			CVE ID : CVE-2019-6171		
20g8_firmw	are			ı	
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could	N/A	O-LEN-20G8- 060919/644
CV Scoring Scale (CVSS)	e 0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171		
20g9_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20G9- 060919/645
20ga_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20GA- 060919/646
20gb_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20GB- 060919/647
20h1_firmw	are			1	

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Des	cription 8	& CVE ID		Patch		N	CIIPC ID
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges cability to up Controller firmware. CVE ID: CV	ons of ol- chat cou- dministr cal acces e Embed signed	N/A		0-Ll 20H 060			
20h2_firmw	are									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller firmware. CVE ID: CV	ons of ol- chat cou- dministr cal acces e Embed signed	N/A		0-Ll 20H 060			
20h4_firmw	are									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges cability to up Controller firmware.	N/A		0-Ll 20H 060				
20h	242		CAE ID : CA	E-2019	-01/1					
20h5_firmw	are			.1		1.		ı		
N/A	19-08-2019	7.2	A vulneraby various BIC ThinkPad so allow a use privileges coability to up Controllery firmware.	ons of ole that cou dministration cal acces e Embed	N/A		0-Ll 20H 060			
CV Scoring Scale (CVSS)	0-1 1-2	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-	.9	9-10

Weakness	Publish Date	cvss		Description	& CVE ID		Patch	1	NCIIPC ID			
			CVE ID	: CVE-201	9-6171							
20h6_firmw	are							•				
N/A	19-08-2019	7.2	various ThinkPa allow a privileg ability t Control firmwa	rability wa BIOS versi ad systems user with a ges or physi to update th ler with un re. CVE-2019	ons of old that cound dministration cal access ne Embed signed	der ld rative s the	N/A	2	-LEN- 0H6- 60919/652			
20h8_firmw	20h8_firmware											
N/A	19-08-2019	7.2	various ThinkPa allow a privileg ability t Control firmwa	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					-LEN- 0H8- 60919/653			
20hm_firmv	vare											
N/A	19-08-2019	7.2	various ThinkPa allow a privileg ability t Control firmwa	rability wa BIOS versi ad systems user with a ges or physi o update th ler with un re. : CVE-201	ons of old that cound dministrated cal access ne Embed signed	N/A	2	-LEN- 0HM- 60919/654				
20hn_firmw	are						ı					
N/A	19-08-2019	7.2	various ThinkPa allow a privileg	rability wa BIOS versi ad systems user with a ses or physi o update th	ons of old that could dministrical acces	der ld rative s the	N/A	2	-LEN- 0HN- 60919/655			
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-	4 4-5	5-6	6-7	7-8	8-9	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware.		
			CVE ID: CVE-2019-6171		
20hs_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20HS- 060919/656
20ht_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.	N/A	O-LEN- 20HT- 060919/657
			CVE ID : CVE-2019-6171		
20hu_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.	N/A	O-LEN- 20HU- 060919/658
			CVE ID: CVE-2019-6171		
20hv_firmw	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could	N/A	0-LEN- 20HV- 060919/659
CV Scoring Scale (CVSS)	0-1 1-2	2 2	3-4 4-5 5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171		
20j1_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20J1- 060919/660
20j2_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20J2- 060919/661
20j4_firmwa	are				
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20J4- 060919/662
20j5_firmwa	are				1

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch		N	CIIPC ID
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad s allow a use privileges of ability to up Controller of firmware. CVE ID: CV	OS versions to service the ser	ons of old that could dministral cal acces e Embed igned	N/A			EN-20J5- 919/663	
20j6_firmwa	ıre									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	ns of old hat could dministral cal acces e Embed igned	N/A			EN-20J6- 919/664		
20j7_firmwa	ire									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	ns of old hat could dministral cal acces e Embed igned	N/A			EN-20J7- 919/665		
20ja_firmwa	ıre									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad seallow a use privileges of ability to up Controller of firmware.	ons of old that could dministral cal acces e Embed	N/A			EN-20JA- 919/666		
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-	9	9-10

Weakness	Publish Date	CVSS	De	scription 8	& CVE ID		Patch	1	NCIIPC ID		
			CVE ID : C	VE-2019	-6171						
20jh_firmwa	are										
N/A	19-08-2019	7.2	A vulnera various B ThinkPad allow a us privileges ability to Controller firmware.	OS versions the systems to systems the systems or with an arms of the systems of	ons of old chat cound dministrated access e Embed signed	N/A		0-LEN-20JH- 060919/667			
20jj_firmware											
N/A	19-08-2019	7.2	various BinnkPad allow a usprivileges ability to Controller firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171)-LEN-20JJ-)60919/668		
20jq_firmwa	are										
N/A	19-08-2019	7.2	various B ThinkPad allow a us privileges ability to Controller firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171)-LEN-20JQ-)60919/669		
20jr_firmwa	re										
N/A	19-08-2019	7.2	A vulnera various B ThinkPad allow a us privileges ability to	OS versions the systems to the serior with a contract or physion o	ons of old that could dministrated acces	der ld rative s the	N/A		O-LEN-20JR- 060919/670		
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	NC	IIPC ID
			Controller firmware. CVE ID : CV							
20ju_firmwa	ire									
N/A	19-08-2019	7.2	A vulneraby various BIO ThinkPad so allow a use privileges of ability to use Controller firmware.	N/A		O-LEN-20JU 060919/67				
20jv_firmwa	ire									
N/A	19-08-2019	7.2	various BIO ThinkPad s allow a use privileges of ability to use Controller firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171						N-20JV- 19/672
20k5_firmwa	are									
N/A	19-08-2019	7.2	A vulneraby various BIC ThinkPad so allow a use privileges cability to use Controller firmware.	N/A			N-20K5- 19/673			
20k6_firmwa	are									
N/A	19-08-2019	7.2	A vulnerab various BIO ThinkPad s	der	N/A			N-20K6- 19/674		
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					
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171							
20kc_firmw	are									
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20KC- 060919/675					
20kd_firmware										
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20KD- 060919/676					
20kl_firmwa	are			1						
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20KL- 060919/677					
20km_firmware										

Weakness	Publish Date	CVSS	Des	cription 8	CVE ID		Patch		NO	CIIPC ID
N/A	19-08-2019	7.2	A vulnerabin various BIC ThinkPad so allow a use privileges of ability to up Controller of firmware. CVE ID: CV	OS versions to the second of t	ns of old hat could dministral cal acces e Embed igned	N/A		0-LE 20KI 0609		
20kn_firmw	are									
N/A	19-08-2019	7.2	A vulnerabing various BIC ThinkPad so allow a use privileges of ability to up Controller with the controller ware.	ns of old hat could dministral cal acces e Embed igned	N/A		O-LE 20KI 0609			
20kq_firmw	are									
N/A	19-08-2019	7.2	A vulnerabing various BIC ThinkPad so allow a use privileges of ability to up Controller with the controll	ns of old hat could dministral cal acces e Embed igned	N/A		O-LE 20K0 0609			
20ks_firmwa	are									
N/A	19-08-2019	7.2	A vulnerabing various BIC ThinkPad so allow a use privileges of ability to up Controller ware.	ons of old that could dministral cal acces e Embed	N/A			IN-20KS- 919/681		
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9	9-10

Weakness	Publish Date	CVSS	De	scription &	& CVE ID		Patch	1	NCIIPC ID	
			CVE ID : C	VE-2019	-6171					
20kt_firmwa	are									
N/A	19-08-2019	7.2	A vulneral various Bl ThinkPad allow a us privileges ability to u Controller firmware.	OS versions of the systems of the sy	ons of old chat cound dministrated access e Embed signed	N/A	2	D-LEN- 20KT- 060919/682		
20ku_firmware										
N/A	19-08-2019	7.2	A vulneral various BI ThinkPad allow a us privileges ability to u Controller firmware.	OS versions of the systems of with a contract or physical properties of the system of	ons of old chat count dministrated access e Embed signed	N/A	2	D-LEN- 20KU- 060919/683		
20kv_firmw	are									
N/A	19-08-2019	7.2	various Bl ThinkPad allow a us privileges ability to u Controller firmware.	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					D-LEN- 20KV- 060919/684	
2012_firmwa	ire									
N/A	19-08-2019	7.2	A vulneral various Bl ThinkPad allow a us privileges ability to u	OS versions the systems to the ser with a contract or physical contract	ons of old that could dministrated al acces	der ld rative s the	N/A		D-LEN-20L2- 060919/685	
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID		
			firn	iware.	with uns /E-2019								
20lh_firmwa	ire												
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					N/A		O-LEN- 20LH- 060919/68			
20lj_firmwa	re												
N/A	19-08-2019	7.2	vari Thi allo priv abil Con firm	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171							EN-20LJ- 919/687		
20lm_firmw	are												
N/A	19-08-2019	7.2	vari Thi allo priv abil Con firm	ious BIC nkPad s w a use vileges c ity to up troller v nware.	ility was OS versic ystems to r with ac or physic odate th with uns	N/A		0-L 20L 060					
20ln_firmwa	ıre												
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could					N/A		0-L 20L 060			
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3	3-4	4-5 5-6 6-7			7-8	8	-9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171					
20lq_firmwa	are							
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN- 20LQ- 060919/690			
20lr_firmwa	ire							
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20LR- 060919/691			
20ls_firmwa	ire							
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171	N/A	O-LEN-20LS- 060919/692			
20lt_firmware								

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges cability to up Controller firmware. CVE ID: CV	OS version ystems to r with accomplysion pdate the with uns	ns of old hat cound dministral cal acces e Embed signed	der ld rative s the	N/A			EN-20LT- 919/693
20lx_firmwa	ire									
N/A	19-08-2019	7.2	various BIO ThinkPad s allow a use privileges o ability to u							EN-20LX- 919/694
20m5_firmw	are									
N/A	19-08-2019	7.2	A vulnerable various BIC ThinkPad so allow a use privileges cability to up Controller firmware.	OS version ystems to r with accomplysion pdate the with uns	ns of old that count dministrated access e Embed signed	der ld rative s the	N/A		0-L 20M 060	
20m (fi	vowo.		CVEID:CI	E-2019	-01/1					
20m6_firmw	аге		A 1	.1.,		1.				
N/A	19-08-2019	7.2	A vulneraby various BIC ThinkPad so allow a use privileges coability to up Controllery firmware.	OS version ystems to with a contract the contract of the contr	ons of old that could dministrated acces the Embed	der ld rative s the	N/A		0-L 20M 060	
CV Scoring Scale (CVSS)	0-1 1-2	2 2	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
			CVE	E ID : CV	E-2019	-6171					
20m7_firmv	vare										
N/A	19-08-2019	7.2	vari Thin allo priv abil Con firm	ous BIC nkPad s w a use rileges o ity to up troller v nware.	lity was S versic ystems t r with ac or physic odate the with uns	ns of ole that count dministral cal acces e Embed signed	der ld rative s the	N/A		O-LI 20M 060	
20m8_firmv	vare		A vulnerability was reported in								
N/A	19-08-2019	7.2	vari Thin allo priv abil Con firm	ous BIC nkPad s w a use rileges o ity to up troller v nware.	llity was OS versic ystems t r with ac or physic odate the with uns	ons of old that count dministrated access e Embed signed	der ld rative s the	N/A		O-LI 20M 060	
20mu_firmv	vare										
N/A	19-08-2019	7.2	vari Thin allo priv abil Con firm	ous BIC nkPad s w a use rileges o ity to up troller v nware.	lity was OS versic ystems to r with ac or physic odate the with uns	ons of old that count dministrated access e Embed signed	der ld rative s the	N/A		O-LI 20M 060	
20mv_firmw	vare										
N/A	19-08-2019	7.2	vari Thii allo priv	ous BIC nkPad s w a use rileges o	llity was OS versic ystems t r with ac or physic odate the	ons of old hat could dministrated al acces	der ld rative s the	N/A		O-LI 20M 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	6-7	7 7-8 8		9	9-10		

Weakness	Publish Date	cvss		Des	cription 8	CVE ID		Patch	1	N	CIIPC ID							
			firm	ware.	with uns E-2019													
20mw_firmv	ware																	
N/A	19-08-2019	7.2	varion Thir allow prives abilication for the firm	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware. CVE ID: CVE-2019-6171 A vulnerability was reported in various BIOS versions of older						0-L 20M 060								
20mx_firmw	are																	
N/A	19-08-2019	7.2	varion Thir allow prives abilication firm	ous BIC akPad s w a use ileges o ty to up troller v ware.	-	ns of ole hat cou dministral al acces e Embed igned	der ld rative s the	N/A		0-L 20M 060								
20n8_firmw	are																	
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could allow a user with administrative privileges or physical access the ability to update the Embedded Controller with unsigned firmware.					N/A		0-L 20N 060								
20n9_firmw	are		CVE ID : CVE-2019-6171															
N/A	19-08-2019	7.2	A vulnerability was reported in various BIOS versions of older ThinkPad systems that could					various BIOS versions of older		various BIOS versions of older		various BIOS versions of older		der	N/A		0-L 20N 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4 4-5 5-6 6-7					7-8		-9	9-10							

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
			allow a use privileges of ability to u Controller firmware.	or physic pdate th with uns	cal acces e Embed signed	s the				
Lexmark										
c925_firmwa	are									
Improper Access Control	28-08-2019	6.4	Various Le Incorrect A CVE ID : CV	ccess Co	ntrol.		http://s pport.le mark.ce /index? ge=con t&id=T; 22&loce =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-C925- 919/705
Integer Overflow or Wraparoun d	28-08-2019	10	Various Le an Integer CVE ID : CV	Overflov	V.	have	http://s pport.le mark.co /index? ge=con t&id=T; 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-C925- 919/706
c950_firmwa	are									
Improper Access Control	28-08-2019	6.4	Various Le Incorrect A CVE ID : CV	ccess Co	ntrol.		http://sport.lemark.com/index?ge=cont&id=T:22&loc=EN&uslocale=_US	ex om ?pa ten E9 ale ser		EX-C950- 919/707
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-	-9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lez an Integer CVE ID : CV	Overflov	V.	have	http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-C950- 919/708
cs51x_firmw	vare									
Improper Access Control	28-08-2019	6.4	Various Le: Incorrect A CVE ID : CV	ccess Co	ntrol.		http:// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-CS51- 919/709
cs748_firmv	vare		<u> </u>							
Improper Access Control	28-08-2019	6.4	Various Le: Incorrect A CVE ID : CV	ccess Co	ntrol.		http:/// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 rale ser	_	EX-CS74- 919/710
Integer Overflow or Wraparoun d	28-08-2019	10	Various Les an Integer CVE ID : CV	have	http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u	ex om ?pa ten E9		EX-CS74- 919/711		
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	6-7	7-8	8-9	9	9-10		

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
								locale= _US	EN		
cs796_firmv	vare										
Improper Access Control	28-08-2019	6.4	Inc	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058				http:/// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 :ale ser		EX-CS79- 919/712
Integer Overflow or Wraparoun d	28-08-2019	10	an l	Various Lexmark products have an Integer Overflow. CVE ID : CVE-2019-9930							EX-CS79- 919/713
e46x_firmwa	are										
Improper Access Control	28-08-2019	6.4	Inc	ious Lex orrect A E ID : CV		http:// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-E46X- 919/714		
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930					http:// pport.le mark.co /index? ge=con	ex om ?pa		EX-E46X- 919/715
CV Scoring Scale	1 1-1 1-1 1-2 1 3-4 1 4-5 1 5-h 1 h-7					6-7	7-8	8-9	9	9-10	

Weakness	Publish Da	te	CVSS		Des	cription 8	CVE ID		Patch	1	N	CIIPC ID
									t&id=T 20&loc =EN&u locale= _US	ale ser		
m3150_firm	ware											
Improper Access Control	28-08-20	19	6.4	Inco	orrect A	xmark pi ccess Co 'E-2019	ntrol.		http://sport.lemark.com/index?ge=cont&id=T22&loc=EN&uslocale=_US	ex om ?pa ten E9 ale ser	O-Li M31 060	
m5155_firm	ware											
Improper Access Control	28-08-20	19	6.4	Inco	orrect A	kmark pi ccess Co 'E-2019	ntrol.		http://s pport.le mark.cc /index? ge=con t&id=T; 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Li M51 060	
Integer Overflow or Wraparoun d	28-08-203	19	10	an I	nteger (xmark pi Overflow 'E-2019	J.	have	http://s pport.le mark.ce /index? ge=con t&id=T; 20&loce =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Li M51 060	
m5163_firm												
Improper	28-08-20	19	6.4	Various Lexmark products have				have	http://	su	0-L	EX-
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
Access Control			Incorrect Access Control. CVE ID: CVE-2019-10058	pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	M516- 060919/719
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- M516- 060919/720
m5170_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- M517- 060919/721
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- M517- 060919/722
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	cvss		Des	cription 8	& CVE ID		Patch	1	NCII	PC ID
ms610de_fir	mware										
Improper Access Control	28-08-2019	6.4	Inco	orrect A	kmark pr ccess Co /E-2019	ntrol.		http://pport.le mark.co /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-LEX MS61- 06091	
ms810de_fir	mware										
Improper Access Control	28-08-2019	6.4	Inco	orrect A	kmark pi ccess Co 'E-2019	ntrol.		http://pport.le mark.co /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-LEX MS81- 06091	
Integer Overflow or Wraparoun d	28-08-2019	10	an I	rious Lexmark products have Integer Overflow. E ID : CVE-2019-9930				http:/// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-LEX MS81- 06091	
ms812de_fir	mware										
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058					http:/// pport.le mark.co /index? ge=con t&id=T	ex om ?pa (ten	0-LEX MS81- 06091	
CV Scoring Scale (CVSS)	0-1	2	2-3 3-4 4-5 5-6 6-7				6-7	7-8 8			9-10

Weakness	Publish Date	cvss	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
							22&loc =EN&u locale= _US	ser		
Integer Overflow or Wraparoun d	28-08-2019	10	Various Le an Integer CVE ID : CV	Overflov	V.	ge=conter t&id=TE9			0-Ll MS8 060	
ms91x_firmv	ware									
Improper Access Control	28-08-2019	6.4	Various Le Incorrect A CVE ID : CV	ccess Co	ntrol.		http:// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS9 060	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Le an Integer CVE ID : CV	have	http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS9 060			
t65x_firmwa	re									
Improper Access Control	28-08-2019	6.4	Various Les Incorrect A CVE ID : CV		http:// pport.le mark.ce	ex		EX-T65X- 919/730		
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
				/index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US						
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-T65X- 060919/731					
w850_firmw	are									
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	0-LEX- W850- 060919/732					
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	0-LEX- W850- 060919/733					
xm51xx_firmware										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- XM51- 060919/734
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- XM51- 060919/735
xm71xx_firm	nware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- XM71- 060919/736
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN	O-LEX- XM71- 060919/737
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
				_US		
cs31x_firmw	vare					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	0-LEX-CS31- 060919/738	
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-CS31- 060919/739	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID : CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	0-LEX-CS31- 060919/740	
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl	O-LEX-CS31- 060919/741	
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4 4-5 5-6 6-7	7-8	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
				ocale=EN_ US	
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	O-LEX-CS31- 060919/742
cs41x_firmw	vare				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX-CS41- 060919/743
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-CS41- 060919/744
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale	O-LEX-CS41- 060919/745
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
							=EN&u locale= _US			
Improper Access Control	28-08-2019	5	Various Let Incorrect A of 2). CVE ID : CV	ccess Co	ntrol (is	http://s pport.le mark.cc /index? ge=con t&id=T: 24&loc =en&us ocale=F	ex om ?pa ten E9 ale		EX-CS41- 919/746	
Improper Access Control	28-08-2019	5	Various Les Incorrect A of 2). CVE ID : CV	ccess Co	ntrol (is	http://s pport.le mark.cc /index? ge=con t&id=T; 24&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-CS41- 919/747	
m1140_firm	ware									
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lea CSRF. CVE ID : CV	-			http://s pport.le mark.co /index? ge=con t&id=T; 21&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll M11 060	
Improper Access Control	28-08-2019	6.4	Various Lex Incorrect A CVE ID : CV	ntrol.		http://s pport.le mark.co /index? ge=con t&id=T	ex om ?pa ten	0-Ll M11 060		
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-	.9	9-10

Weakness	Publish Date	cvss		Desc	cription 8	k CVE ID		Patch	1	N	CIIPC ID						
								22&loc =EN&u locale= _US	ser								
Integer Overflow or Wraparoun d	28-08-2019	10	an Ir	nteger (xmark pr Overflov 'E-2019	V.	http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll M11 060								
Improper Access Control	28-08-2019	5	Inco of 2)	rrect A).	xmark pi ccess Co Y E-2019	ntrol (is	http:// pport.le mark.ce /indexi ge=con t&id=T 24&loc =en&us ocale=H US	ex om ?pa ten E9 ale	0-Ll M11 060								
Improper Access Control	28-08-2019	5	Inco of 2)	rrect A	roducts ntrol (is		http:// pport.le mark.ce /index? ge=con t&id=T 24&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll M11 060								
m1145_firm	ware																
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057		CSRF.		CSRF.		CSRF.		CSRF.		ma			0-Ll M11 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9	9-10						

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch)	N	CIIPC ID			
							t&id=Ti 21&loca =EN&ua locale=1	ale ser					
Improper Access Control	28-08-2019	6.4	Various Le Incorrect A CVE ID : CV	ccess Co	ntrol.		http://s pport.le mark.cc /index? ge=con t&id=Ti 22&loca =EN&us locale=: _US	ex om Ppa ten E9 ale ser	0-Ll M11 060				
Integer Overflow or Wraparoun d	28-08-2019	10	Various Le an Integer CVE ID : CV	Overflov	V.	have	http://s pport.le mark.co /index? ge=con t&id=T! 20&loca =EN&us locale=:	ex om om opa ten E9 ale ser	0-Ll M11 060				
Improper Access Control	28-08-2019	5	Various Le Incorrect A of 2). CVE ID : CV	access Co	ontrol (is		http://s pport.le mark.co /index? ge=con t&id=T] 24&locs =en&us ocale=E	ex om om opa ten E9 ale serl	0-Ll M11 060				
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935			Incorrect Access Control (issue 2 of 2).		Incorrect Access Control (issue 2 of 2).			su ex om 'pa ten	0-Ll M11 060	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	4-5	5-6	6-7	7-8	8-	-9	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				t&id=TE9 24&locale =EN&user locale=EN _US	
m3150dn_fi	rmware				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX- M315- 060919/758
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- M315- 060919/759
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- M315- 060919/760
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2).	http://su pport.lex mark.com /index?pa	O-LEX- M315- 060919/761
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
			CVI	E ID : CV	Æ-2019	-9934		ge=con t&id=T 24&loc =en&us ocale=F US	E9 ale serl		
Improper Access Control	28-08-2019	5	Inco	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935				http://sport.lemark.com/index?ge=cont&id=T24&loc=EN&uslocale=_US	ex om ?pa ten E9 ale ser	0-Ll M31 060	
m5163dn_fi	rmware										
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	CSF	Various Lexmark products have CSRF. CVE ID : CVE-2019-10057 pport.lex mark.com /index?pa ge=content t&id=TE9 21&locale =EN&use locale=EN _US				om ?pa ten E9 ale ser	0-Ll M51 060		
Improper Access Control	28-08-2019	6.4	Inc	orrect A	kmark p ccess Co /E-2019	ntrol.		http://s pport.le mark.co /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser EN	0-Ll M51 060	
Integer Overflow or Wraparoun	28-08-2019	10	Various Lexmark products have an Integer Overflow.		have	http://s pport.le mark.co	ex	O-L M51			
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		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
d			CV	E ID : CV	/E-2019	-9930		/indexinge=contwiction two distributions of the control of the con	ten E9 ale ser	060	919/765
Improper Access Control	28-08-2019	5	Inc of 2	rious Lex correct A 2). E ID : CV	ccess Co	ontrol (is	http:// pport.le mark.ce /index? ge=con t&id=T 24&loc =en&us ocale=H US	ex om ?pa ten E9 ale	0-Li M51 060		
Improper Access Control	28-08-2019	5	Inc of 2	rious Lex correct A 2). E ID : CV	ccess Co	ontrol (is		http:// pport.le mark.ce /index? ge=con t&id=T 24&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-L M51 060	
ms310_firm	ware										
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	CS	rious Lez RF. E ID : CV				http:// pport.le mark.ce /indexis ge=con t&id=T 21&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-L MS3 060	
Improper Access	28-08-201	6.4	Vai	Various Lexmark products have					su ex	O-L MS3	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8		-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			Incorrect Access Control. CVE ID: CVE-2019-10058	mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	060919/769
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MS31- 060919/770
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	O-LEX- MS31- 060919/771
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	O-LEX- MS31- 060919/772
ms312_firm	ware				

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

Weakness	Publish Date	cvss	D	escription 8	& CVE ID		Patch		N	CIIPC ID
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	CSRF.	exmark p CVE-2019			http://s pport.le mark.co /index? ge=cont t&id=Tl 21&loca =EN&us locale=l	ex om pa ten E9 ale ser	O-LI MS3 060	
Improper Access Control	28-08-2019	6.4	Incorrect	exmark p Access Co C VE-201 9	ntrol.	http://s pport.le mark.co /index? ge=cont t&id=Tl 22&loca =EN&us locale=l _US	ex om pa ten E9 ale	0-Ll MS3 060		
Integer Overflow or Wraparoun d	28-08-2019	10	an Intege	exmark p r Overflov C VE-201 9	V.	have	http://s pport.le mark.co /index? ge=cont t&id=Tl 20&loca =EN&us locale=l	ex om opa ten E9 ale ser	0-Ll MS3 060	
Improper Access Control	28-08-2019	5	Incorrect of 2).	exmark p Access Co CVE-2019	ontrol (is		http://s pport.le mark.co /index? ge=cont t&id=TI 24&loca =en&us ocale=E	ex om pa ten E9 ale erl	0-Ll MS3 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-	9	9-10

Weakness	Publish Date	CVSS		Description	on &	CVE ID		Patch	۱	N	CIIPC ID
Improper Access Control	28-08-2019	5	Incorred of 2).	Lexmar ct Access : CVE-20	s Co	ntrol (i	http:// pport.le mark.ce /index? ge=con t&id=T 24&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS3 060		
ms315_firm	ware										
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	CSRF.	Lexmar	•		http:// pport.le mark.co /index? ge=con t&id=T 21&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS3 060		
Improper Access Control	28-08-2019	6.4	Incorre	Lexmar ct Access	s Co	ntrol.		http:/// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS3 060	
Integer Overflow or Wraparoun d	28-08-2019	10	an Integ	Lexmar ger Overf	flow	7.	have	http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale=	ex om ?pa ten E9 ale ser	0-Ll MS3 060	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	!-3 3-4	5-6	6-7	7-8	8-	9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	NCIIPC ID	
				_US	
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	O-LEX- MS31- 060919/781
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	O-LEX- MS31- 060919/782
ms317_firm	ware				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX- MS31- 060919/783
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058 http://s pport.le mark.co /index? ge=cont t&id=TE 22&loca =EN&us		O-LEX- MS31- 060919/784
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				locale=EN _US	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MS31- 060919/785
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	O-LEX- MS31- 060919/786
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	O-LEX- MS31- 060919/787
ms410_firm	ware				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale	O-LEX- MS41- 060919/788
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	NO	CIIPC ID	
							=EN&us locale=1 _US				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058			Incorrect Access Control.		http://s pport.le mark.co /index? ge=con t&id=Tl 22&loca =EN&us locale=1	ex om om opa ten ten E9 ale	0-LE MS4 0609	
Integer Overflow or Wraparoun d	28-08-2019	10	an Integer	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930					0-LE MS4 0609		
Improper Access Control	28-08-2019	5	Various Lez Incorrect A of 2). CVE ID : CV	http://s pport.le mark.co /index? ge=con t&id=Ti 24&loca =en&us ocale=E	ex om Ppa ten E9 ale	O-LE MS4 0609					
Improper Access Control	28-08-2019	5	Various Lex Incorrect A of 2). CVE ID : CV		http://s pport.le mark.co /index? ge=cont t&id=Tl 24&loca	ex om 'pa ten E9	0-LE MS4 0609				
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	6-7	7-8	8-	9	9-10			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
				=EN&user locale=EN _US	
ms415_firm	ware				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX- MS41- 060919/793
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MS41- 060919/794
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MS41- 060919/795
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9	O-LEX- MS41- 060919/796
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	cvss		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
								24&loc =en&us ocale=I US	serl		
Improper Access Control	28-08-2019	5	Inc of 2	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935					ten L	0-Ll MS4 060	
ms417_firmv	ware										
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	CSF	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057					ten	0-Ll MS4 060	
Improper Access Control	28-08-2019	6.4	Inc	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058					ten F9	0-Ll MS4 060	
Integer Overflow or Wraparoun d	28-08-2019	10	an I	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930					om	O-L MS4 060	
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3	3 3-4 4-5 5-6 6-7				7-8	8-	9	9-10

Weakness	Publish Date	cvss		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
						t&id=T 20&loc =EN&u locale= _US	ale ser				
Improper Access Control	28-08-2019	5	Inco of 2	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934					su ex om ?pa ten E9 ale serl	0-Ll MS4 060	
Improper Access Control	28-08-2019	5	Inco of 2	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935					su ex om ?pa ten E9 ale ser	0-Ll MS4 060	
ms51x_firm	ware										
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	CSR	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057					su ex om ?pa ten E9 ale ser EN	0-Ll MS5 060	
Improper Access Control	28-08-2019	6.4	Inco	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058					su ex om ?pa	0-Ll MS5 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Dat	cvs	S	Des	Patch	1	N	CIIPC ID				
								ge=con t&id=T 22&loc =EN&u locale= _US	E9 ale ser			
Integer Overflow or Wraparoun d	28-08-201	9 10	an	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930					su ex om ?pa ten E9 ale ser EN	0-Ll MS5 060		
Improper Access Control	28-08-201	5	In of	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934					su ex om ?pa ten E9 ale serl	0-Ll MS5 060		
Improper Access Control	28-08-201	5	In of	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935					su ex om ?pa ten E9 ale ser EN	0-Ll MS5 060		
ms610dn_fii	rmware											
Cross-Site Request Forgery	28-08-201	9 4.3		-		Various Lexmark products have CSRF.		have	http:// pport.le mark.ce	ex	O-L	
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
(CSRF)			CVE ID : CVE-2019-10057	/index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	060919/808
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MS61- 060919/809
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MS61- 060919/810
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	O-LEX- MS61- 060919/811
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2).	http://su pport.lex mark.com	O-LEX- MS61- 060919/812
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2019-9935	/index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US		
ms617_firm	ware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX- MS61- 060919/813	
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MS61- 060919/814	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MS61- 060919/815	
Improper Access	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1	http://su pport.lex	O-LEX- MS61-	
CV Scoring Scale (CVSS)	0-1 1-2	2 2	3-4 4-5 5-6 6-7	7-8	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Control			of 2). CVE ID: CVE-2019-9934	mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	060919/816
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	O-LEX- MS61- 060919/817
ms71x_firm	ware				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX- MS71- 060919/818
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MS71- 060919/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MS71- 060919/820
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	O-LEX- MS71- 060919/821
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	O-LEX- MS71- 060919/822
ms810_firm	ware				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN	O-LEX- MS81- 060919/823
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	cvss	Description & CVE ID						N	CIIPC ID									
				_US															
Improper Access Control	28-08-2019	6.4	Incorrect A	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058			Incorrect Access Control.			Incorrect Access Control.			Incorrect Access Control.			http://s pport.le mark.co /index? ge=con t&id=Tl 22&loca =EN&us locale=1	ex om pa ten E9 ale	0-LI MS8 060	
Integer Overflow or Wraparoun d	28-08-2019	10	an Integer	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930						EX- 1- 919/825									
Improper Access Control	28-08-2019	5	Incorrect A of 2).	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934					0-LI MS8 060										
Improper Access Control	28-08-2019	5	Various Lez Incorrect A of 2). CVE ID : CV		http://s pport.le mark.co /index? ge=con t&id=Tl 24&loca =EN&us locale=l	ex om pa ten E9 ale	0-LI MS8 060												
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	6-7	7-8	8-	.9	9-10											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				_US	
ms811_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX- MS81- 060919/828
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MS81- 060919/829
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MS81- 060919/830
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl	O-LEX- MS81- 060919/831
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	Des	cription 8	Patch	1	NCIIPC ID		
							ocale=I US	EN_	
Improper Access Control	28-08-2019	5	Various Le Incorrect A of 2). CVE ID : C	Access Co	ntrol (is		http:// pport.le mark.ce /index/ ge=con t&id=T 24&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	O-LEX- MS81- 060919/832
ms812_firm	ware								
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Le CSRF. CVE ID : C			have	http:// pport.le mark.cc /indexi ge=con t&id=T 21&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-LEX- MS81- 060919/833
Improper Access Control	28-08-2019	6.4	Various Le Incorrect A CVE ID : C	Access Co	ntrol.		http:// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	O-LEX- MS81- 060919/834
Integer Overflow or Wraparoun d	28-08-2019	10	Various Le an Integer CVE ID : C	V.	http:// pport.le mark.ce /indexi ge=con t&id=T 20&loc	ex om (?pa (!) ten (E9)	0-LEX- MS81- 060919/835		
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & C	Patch	NCIIPC ID	
					=EN&user locale=EN _US	
Improper Access Control	28-08-2019	5	Various Lexmark pro- Incorrect Access Cont of 2). CVE ID : CVE-2019-9	crol (issue 1	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	MS81- 060919/836
Improper Access Control	28-08-2019	5	Various Lexmark pro Incorrect Access Cont of 2). CVE ID : CVE-2019-9	crol (issue 2	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	MS81- 060919/837
ms817_firm	ware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark pro CSRF. CVE ID : CVE-2019-1	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	MS81- 060919/838	
Improper Access Control	28-08-2019	6.4	Various Lexmark pro Incorrect Access Cont CVE ID : CVE-2019-1	crol.	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9	1000717/037
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		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
								22&loc =EN&u locale= _US	ser		
Integer Overflow or Wraparoun d	28-08-2019	10	an Ir	iteger (xmark pr Overflov 'E-2019		have	http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS8 060	
Improper Access Control	28-08-2019	5	Inco of 2)	rrect A	_	roducts introl (is		http:// pport.le mark.ce /indexis ge=con t&id=T 24&loc =en&us ocale=H US	ex om ?pa ten E9 ale serl	0-Ll MS8 060	
Improper Access Control	28-08-2019	5	Inco of 2)	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935			http:// pport.le mark.ce /index? ge=con t&id=T 24&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS8 060		
ms818_firm	ware										
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057					http:// pport.le mark.ce /index? ge=con	ex om ?pa	0-Ll MS8 060	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3 3-4 4-5 5-6 6-7			6-7	7-8 8		.9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
							t&id=T 21&loc =EN&u locale= _US	ale ser		
Improper Access Control	28-08-2019	6.4	Various Lea Incorrect A CVE ID : CV	ccess Co	ntrol.		http://s pport.le mark.cc /index? ge=con t&id=T; 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-LI MS8 060	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Les an Integer (CVE ID : CV	Overflov	V.	have	http://s pport.le mark.cc /index? ge=con t&id=T; 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MS8 060	
Improper Access Control	28-08-2019	5	Various Lex Incorrect A of 2). CVE ID : CV	http://s pport.le mark.ce /index? ge=con t&id=T; 24&loce =en&us ocale=E	ex om ?pa ten E9 ale	0-Ll MS8 060				
Improper Access Control	28-08-2019	5	Various Les Incorrect A of 2). CVE ID : CV	ccess Co	ntrol (is		http://s pport.le mark.co /index? ge=con	ex om ?pa	0-LI MS8 060	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	4-5	5-6	6-7	7-8	8-	.9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				t&id=TE9 24&locale =EN&user locale=EN _US	
xm1135_firm	nware				
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 21&locale =EN&user locale=EN _US	O-LEX- XM11- 060919/848
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- XM11- 060919/849
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- XM11- 060919/850
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2).	http://su pport.lex mark.com /index?pa	O-LEX- XM11- 060919/851
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
			CVE I	D : CV	Æ-2019	-9934		ge=con t&id=T 24&loc =en&us ocale=H US	E9 ale serl		
Improper Access Control	28-08-2019	5	Incorrof 2).	rect A	kmark p ccess Co YE-2019	ontrol (is		http:/// pport.le mark.cc /index? ge=con t&id=T 24&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	O-Ll XM1 060	
c734_firmwa	are										
Improper Access Control	28-08-2019	6.4	Incori	rect A	kmark p ccess Co /E-2019	ntrol.		http:/// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-C734- 919/853
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930					http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US		_	EX-C734- 919/854
c736_firmwa											
Improper	28-08-2019	6.4	Vario	us Lex	kmark p	roducts	have	http://	su	O-L	EX-C736-
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	cvss	Des	cription 8	CVE ID		Patch	1	N	CIIPC ID
Access Control			Incorrect A CVE ID : CV				pport.le mark.co /index? ge=con t&id=T 22&loc =EN&u locale= _US	om ?pa ten E9 ale ser	060	919/855
Integer Overflow or Wraparoun d	28-08-2019	10	Various Les an Integer (CVE ID : CV	Overflov	J.	have	http:// pport.le mark.co /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-C736- 919/856
c746_firmwa	are									
Improper Access Control	28-08-2019	6.4	Various Lex Incorrect A CVE ID : CV	ccess Co	ntrol.		http:// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-C746- 919/857
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930				http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-C746- 919/858
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-	.9	9-10

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	n	N	CIIPC ID
c748_firmwa	are										
Improper Access Control	28-08-2019	6.4	Inco	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058				http:// pport.le mark.ce /index/ ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa tten E9 :ale ser		EX-C748- 919/859
Integer Overflow or Wraparoun d	28-08-2019	10	an I	nteger (kmark p Overflov /E-2019		have	http:// pport.le mark.ce /index/ ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa tten E9 cale ser		EX-C748- 919/860
c792_firmwa	are										
Improper Access Control	28-08-2019	6.4	Inco	orrect A	ccess Co	roducts ontrol. -10058		http:// pport.le mark.ce /indexi ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa tten E9 cale ser		EX-C792- 919/861
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930				http:// pport.le mark.ce /indexi ge=con t&id=T 20&loc =EN&u	ex om ?pa ten E9		EX-C792- 919/862	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3 3-4 4-5 5-6 6-7			6-7	7-8	8-9	9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				locale=EN _US	
x86x_firmwa	are				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-X86X- 060919/863
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-X86X- 060919/864
x925_firmwa	are				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-X925- 060919/865
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten	O-LEX-X925- 060919/866
CV Scoring Scale (CVSS)	0-1 1-7	2 2	-3 3-4 4-5 5-6 6-7 261	7-8 8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				t&id=TE9 20&locale =EN&user locale=EN _US	
x95x_firmwa	are				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-X95X- 060919/867
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-X95X- 060919/868
xm3150_firm	nware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- XM31- 060919/869
Integer Overflow or	28-08-2019	10	Various Lexmark products have an Integer Overflow.	http://su pport.lex	O-LEX- XM31-
CV Scoring Scale (CVSS)	0-1 1-2	2 2	3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d			CVE ID : CVE-2019-9930	mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	060919/870
xm91x_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- XM91- 060919/871
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- XM91- 060919/872
xs548_firmv	vare				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN	0-LEX-XS54- 060919/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				_US	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-XS54- 060919/874
xs748_firmw	vare				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	0-LEX-XS74- 060919/875
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	0-LEX-XS74- 060919/876
xs79x_firmw	are				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9	O-LEX-XS79- 060919/877
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	-9 9-10

Weakness	Publish Date	CVSS		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
								22&loc =EN&u locale= _US	ser		
Integer Overflow or Wraparoun d	28-08-2019	9 10	an l	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930					su ex om ?pa ten E9 ale ser EN		EX-XS79- 919/878
xs925_firmv	vare										
Improper Access Control	28-08-2019	6.4	Inc	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058				http:// pport.le mark.ce /indexi ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser		EX-XS92- 919/879
Integer Overflow or Wraparoun d	28-08-2019	9 10	an l	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930				http:// pport.le mark.ce /index/ ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	_	EX-XS92- 919/880
xs95x_firmw	vare										
Improper Access Control	28-08-2019	6.4	Inc	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058					su ex om		EX-XS95- 919/881
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
				/index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-XS95- 060919/882
6500e_firmw	vare				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-6500- 060919/883
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-6500- 060919/884
cx310_firmw	are				

4-5

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS		Des	cription 8	k CVE ID		Patch	1	N	CIIPC ID
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	CSRF.	Various Lexmark products have CSRF. CVE ID: CVE-2019-10057							EX-CX31- 919/885
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058					http://s pport.le mark.co /index? ge=con t&id=Tl 22&loca =EN&us locale=1	ex om pa ten E9 ale ser		EX-CX31- 919/886
Integer Overflow or Wraparoun d	28-08-2019	10	an Int	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930				http://s pport.le mark.co /index? ge=con t&id=Tl 20&loca =EN&us locale=l	ex om pa ten E9 ale ser		EX-CX31- 919/887
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934					http://s pport.le mark.co /index? ge=con t&id=Tl 24&locs =en&us ocale=E	ex om pa ten E9 ale		EX-CX31- 919/888
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	Des	cription 8	& CVE ID		Patch	۱	N	CIIPC ID
Improper Access Control	28-08-2019	5	Incorrect A of 2).	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935						EX-CX31- 919/889
mx31x_firm	ware									
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Le CSRF. CVE ID : C	-			http://s pport.le mark.co /index? ge=con t&id=T! 21&locs =EN&us locale=:	ex om ?pa ten E9 ale ser	0-LI MX3 0609	
Improper Access Control	28-08-2019	6.4	Incorrect A	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058				ten F9	0-LI MX3 0609	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Le an Integer CVE ID : C	http://s pport.le mark.co /index? ge=con t&id=Tl 20&locs =EN&us locale=	ex om ?pa ten E9 ale ser	0-LE MX3 0609				
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
				_US	
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). CVE ID: CVE-2019-9934	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =en&userl ocale=EN_ US	O-LEX- MX31- 060919/893
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). CVE ID: CVE-2019-9935	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 24&locale =EN&user locale=EN _US	O-LEX- MX31- 060919/894
mx410_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MX41- 060919/895
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user	O-LEX- MX41- 060919/896
CV Scoring Scale (CVSS)	0-1 1-	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				locale=EN _US	
mx510_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MX51- 060919/897
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MX51- 060919/898
mx511_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MX51- 060919/899
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten	O-LEX- MX51- 060919/900
CV Scoring Scale (CVSS)	0-1 1-7	2 2	3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
				t&id=TE9 20&locale =EN&user locale=EN _US				
mx610_firm	ware							
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MX61- 060919/901			
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MX61- 060919/902			
mx611_firm	ware							
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MX61- 060919/903			
Integer Overflow or	28-08-2019	10	Various Lexmark products have an Integer Overflow. http://su pport.lex MX61-					
CV Scoring Scale (CVSS)	0-1 1-2	2 2	-3 3-4 4-5 5-6 6-7	7-8	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d			CVE ID : CVE-2019-9930	mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	060919/904
mx6500e_fin	rmware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MX65- 060919/905
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MX65- 060919/906
mx71x_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN	O-LEX- MX71- 060919/907

4-5

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				_US	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MX71- 060919/908
mx81x_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX- MX81- 060919/909
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX- MX81- 060919/910
mx91x_firm	ware				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9	O-LEX- MX91- 060919/911
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4 4-5 5-6 6-7	7-8 8	9-10

Weakness	Publish Date	cvss	Des	cription 8	& CVE ID		Patch	1	N	CIIPC ID
							22&loc =EN&u locale= _US	ser		
Integer Overflow or Wraparoun d	28-08-2019	10	Various Le an Integer CVE ID : CV	Overflov	V.	have	http:// pport.le mark.ce /index? ge=con t&id=T 20&loc =EN&u locale= _US	ex om ?pa ten E9 ale ser	0-Ll MX9 060	
x46x_firmwa	are									
Improper Access Control	28-08-2019	6.4	Various Le Incorrect A CVE ID : CV	ccess Co	ntrol.		http:// pport.le mark.ce /index? ge=con t&id=T 22&loc =EN&u locale= _US	ex om ?pa ten E9 cale ser		EX-X46X- 919/913
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930				http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US			EX-X46X- 919/914
x548_firmwa	are									
Improper Access Control	28-08-2019	6.4	Various Les Incorrect A CVE ID : CV	http://su pport.lex mark.com		0-LEX-X548- 060919/915				
CV Scoring Scale (CVSS)	0-1 1-	2 2	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-X548- 060919/916
x65x_firmwa	are				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-X65X- 060919/917
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-X65X- 060919/918
x73x_firmwa	are			•	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	O-LEX-X73X- 060919/919
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN _US	O-LEX-X73X- 060919/920
x74x_firmwa	are				
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 22&locale =EN&user locale=EN _US	0-LEX-X74X- 060919/921
Integer Overflow or Wraparoun d	28-08-2019	10	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930	http://su pport.lex mark.com /index?pa ge=conten t&id=TE9 20&locale =EN&user locale=EN	0-LEX-X74X- 060919/922
CV Scoring Scale (CVSS)	0-1 1-3	2 2	-3 3-4 4-5 5-6 6-7	7-8 8	-9 9-10

Weakness	Publish Date	CVSS	Des	Patch	ı	N	CIIPC ID			
						_US				
x792_firmwa	are									
Improper Access Control	28-08-2019	6.4	Incorrect A	Various Lexmark products have Incorrect Access Control. CVE ID: CVE-2019-10058						EX-X792- 919/923
Integer Overflow or Wraparoun d	28-08-2019	10	an Integer	Various Lexmark products have an Integer Overflow. CVE ID: CVE-2019-9930						EX-X792- 919/924
Linux										
linux_kerne										
Double Free	23-08-2019	10	drivers/ne- _usb.c in th 5.2.9 has a crafted USE may be ren usbredir). CVE ID : CV	e Linux l Double I 3 device note via	kernel tl Free via traffic (v usbip or	nrough which	N/A			N-LINU- 919/925
Out-of- bounds Read	23-08-2019	10	drivers/me usb/techni kernel thro of-bounds i device traff remote via CVE ID : CV	sat-usb2 ugh 5.2. read via ic (whic usbip or	.c in the 9 has an crafted h may b usbred	N/A			N-LINU- 919/926	
CV Scoring Scale (CVSS)	0-1 1-3	2 2	3-4	4-5	5-6	6-7	7-8	8-	9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-08-2019	4.6	parse_audio_mixer_unit in sound/usb/mixer.c in the Linux kernel through 5.2.9 mishandles a short descriptor, leading to out-of-bounds memory access. CVE ID: CVE-2019-15117	N/A	O-LIN-LINU- 060919/927
Uncontrolle d Resource Consumptio n	16-08-2019	4.9	check_input_term in sound/usb/mixer.c in the Linux kernel through 5.2.9 mishandles recursion, leading to kernel stack exhaustion. CVE ID: CVE-2019-15118	N/A	O-LIN-LINU- 060919/928
Use After Free	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/v4l2-core/v4l2-dev.c driver because drivers/media/radio/radio-raremono.c does not properly allocate memory. CVE ID: CVE-2019-15211	N/A	O-LIN-LINU- 060919/929
Double Free	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.1.8. There is a double-free caused by a malicious USB device in the drivers/usb/misc/rio500.c driver. CVE ID: CVE-2019-15212	N/A	O-LIN-LINU- 060919/930
Use After Free	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.2.3. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/dvb-usb/dvb-usb-init.c driver. CVE ID: CVE-2019-15213	N/A	O-LIN-LINU- 060919/931

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-08-2019	4.7	An issue was discovered in the Linux kernel before 5.0.10. There is a use-after-free in the sound subsystem because card disconnection causes certain data structures to be deleted too early. This is related to sound/core/init.c and sound/core/info.c. CVE ID: CVE-2019-15214	N/A	0-LIN-LINU- 060919/932
Use After Free	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/cpia2/cpia2_usb.c driver. CVE ID: CVE-2019-15215	N/A	O-LIN-LINU- 060919/933
NULL Pointer Dereferenc e	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.0.14. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/yurex.c driver. CVE ID: CVE-2019-15216	N/A	O-LIN-LINU- 060919/934
NULL Pointer Dereferenc e	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.2.3. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/zr364xx/zr364xx.c driver. CVE ID: CVE-2019-15217	N/A	O-LIN-LINU- 060919/935
NULL Pointer Dereferenc e	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/siano/smsus	N/A	O-LIN-LINU- 060919/936

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			b.c driver.		
			CVE ID : CVE-2019-15218		
NULL Pointer Dereferenc e	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/sisusbvga/sisu sb.c driver. CVE ID: CVE-2019-15219	N/A	O-LIN-LINU- 060919/937
Use After Free	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.2.1. There is a use-after-free caused by a malicious USB device in the drivers/net/wireless/intersil/p5 4/p54usb.c driver. CVE ID: CVE-2019-15220	N/A	O-LIN-LINU- 060919/938
NULL Pointer Dereferenc e	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.1.17. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/line6/pcm.c driver. CVE ID: CVE-2019-15221	N/A	O-LIN-LINU- 060919/939
NULL Pointer Dereferenc e	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.2.8. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/helper.c (motu_microbookii) driver. CVE ID: CVE-2019-15222	N/A	O-LIN-LINU- 060919/940
NULL Pointer Dereferenc e	19-08-2019	4.9	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/line6/driver.c driver.	N/A	O-LIN-LINU- 060919/941

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15223		
Use After Free	20-08-2019	7.2	In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, was incorrectly backported to the earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that was intended to be fixed by backporting. Specifically, by adding to a write queue between disconnection and reconnection, a local attacker can trigger multiple use-after-free conditions. This can result in a kernel crash, or potentially in privilege escalation. NOTE: this affects (for example) Linux distributions that use 4.9.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.14.139.	N/A	O-LIN-LINU- 060919/942
NULL Pointer Dereferenc e	20-08-2019	4.9	An issue was discovered in the Linux kernel through 5.2.9. There is a NULL pointer dereference caused by a malicious USB device in the ath6kl_usb_alloc_urb_from_pipe function in the drivers/net/wireless/ath/ath6kl /usb.c driver. CVE ID: CVE-2019-15290	N/A	0-LIN-LINU- 060919/943
NULL Pointer Dereferenc e	20-08-2019	4.9	An issue was discovered in the Linux kernel through 5.2.9. There is a NULL pointer dereference caused by a malicious USB device in the flexcop_usb_probe function in the	N/A	O-LIN-LINU- 060919/944
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		Descr	iption 8	CVE ID		Patch	1	NCIIPC ID	
			drivers -usb.c			/b2c2/f	lexcop				
			CVE ID	: CVI	E-2019	-15291					
Use After Free	21-08-2019	10	Linux k is a use atalk_p net/app net/app	kernel e-after proc_e pletal pletal pletal	before r-free ii xit, rela k/atall k/ddp. k/sysc	nted to x_proc.c,	N/A	_	-LIN-LINU- 60919/945		
Out-of- bounds Read	27-08-2019	7.8	Linux k is an ou in _xfr will cau becaus	before bounds licy_un enial of fy_new rm_use	vered in 5.0.19. array a link, whe service, policy_ir.c mish	N/A	_	-LIN-LINU- 50919/946			
			CVE ID	: CVI	E-2019	-15666					
Motorola											
cx2l_mwr04	l_firmware										
Improper Input Validation	23-08-2019	7.8	An issue was discovered in OpenWrt libuci (aka Library for the Unified Configuration Interface) as used on Motorola CX2L MWR04L 1.01 and C1 MWR03 1.01 devices. /tmp/.uci/network locking is mishandled after reception of a long SetWanSettings command, leading to a device hang.					N/A	C	-MOT- K2L- 50919/947	
			CVE ID : CVE-2019-15513								
c1_mwr03_fi	rmware								ı		
Improper Input Validation	23-08-2019	7.8	An issue was discovered in OpenWrt libuci (aka Library for the Unified Configuration Interface) as used on Motorola					N/A	C	O-MOT- C1_M- 060919/948	
CV Scoring Scale	0-1 1-		2-3 3		4-5	5-6	6-7	7-8	8-9		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CX2L MWR04L 1.01 and C1 MWR03 1.01 devices. /tmp/.uci/network locking is mishandled after reception of a long SetWanSettings command, leading to a device hang. CVE ID: CVE-2019-15513		
Paloaltonety	works				
pan-os					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-08-2019	10	Memory corruption in PAN-OS 7.1.24 and earlier, PAN-OS 8.0.19 and earlier, PAN-OS 8.1.9 and earlier, and PAN-OS 9.0.3 and earlier will allow a remote, unauthenticated user to craft a message to Secure Shell Daemon (SSHD) and corrupt arbitrary memory. CVE ID: CVE-2019-1580	https://se curityadvi sories.pal oaltonetw orks.com/ home/det ail/159	O-PAL-PAN 060919/949
Improper Input Validation	23-08-2019	7.5	Mitigation bypass in PAN-OS 7.1.24 and earlier, PAN-OS 8.0.19 and earlier, PAN-OS 8.1.9 and earlier, and PAN-OS 9.0.3 and earlier will allow a remote, unauthenticated user to execute arbitrary code by crafting a malicious message. CVE ID: CVE-2019-1581	https://se curityadvi sories.pal oaltonetw orks.com/ home/det ail/160	O-PAL-PAN 060919/950
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-08-2019	6.5	Memory corruption in PAN-OS 8.1.9 and earlier, and PAN-OS 9.0.3 and earlier will allow an administrative user to cause arbitrary memory corruption by rekeying the current client interactive session. CVE ID: CVE-2019-1582	https://se curityadvi sories.pal oaltonetw orks.com/ home/det ail/161	O-PAL-PAN 060919/951
Tp-link					

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

Weakness	Publish Date	CVSS	D	escription 8	Patch	1	NCIIPC ID		
tl-wr840n_fi	rmware		<u> </u>						
Improper Input Validation	22-08-2019	6.5	TP-Link with firm is vulnera execution an IP add	route fund L-WR840 ware throuble to rend via a craf ress input	N v4 roo ugh 0.9. note cod ted payl field.	iter 1 3.16 e oad in	N/A		0-TPTL-W- 060919/952
zebra									
220xi4_firm	ware								
N/A	20-08-2019	5	Versions, shipped was accessored functions applied, so could be network and the pan array includes for the pris retriev have phy panel of tagsscode	Zebra Industrial Printers All Versions, Zebra printers are shipped with unrestricted end- user access to front panel options. If the option to use a passcode to limit the functionality of the front panel is applied, specially crafted packets could be sent over the same network to a port on the printer and the printer will respond with an array of information that includes the front panel passcode for the printer. Once the passcode is retrieved, an attacker must have physical access to the front panel of the printer to enter the passcode to access the full functionality of the front panel.					O-ZEB-220X- 060919/953
zt220_firmw	are						T		
N/A	20-08-2019	5	Versions, shipped waser acceoptions. I passcode functiona	ustrial Pr Zebra pri vith unres ss to front f the optic to limit th lity of the pecially c	nters are tricted e panel on to use e front pa	N/A		O-ZEB-ZT22- 060919/954	
CV Scoring Scale (CVSS)	0-1 1	-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Des	cription 8	& CVE ID		Patcl	h	N	CIIPC ID
			netw and t an ar inclu for th is ret have pane passo funct	rork to the pri- des th ne prin rieved physic l of the code to	a port on the port of the port	resportion that panel pare the pare to the to enter the full front p					
zt230_firmv	vare										
N/A	20-08-2019	5	Versishippuser option passo funct application and tan arinclu for this retails have passon	Zebra Industrial Printers All Versions, Zebra printers are shipped with unrestricted end- user access to front panel options. If the option to use a passcode to limit the functionality of the front panel is applied, specially crafted packets could be sent over the same network to a port on the printer and the printer will respond with an array of information that includes the front panel passcode for the printer. Once the passcode is retrieved, an attacker must have physical access to the front panel of the printer to enter the passcode to access the full functionality of the front panel.							EB-ZT23- 919/955
zt410_firmv	vare								<u>_</u>		
N/A	20-08-2019	5	Zebra Industrial Printers All Versions, Zebra printers are shipped with unrestricted end- user access to front panel options. If the option to use a								
CV Scoring Scale	e 0-1 1-7	2 2					6-7	7-8	8-9		9-10

Weakness	Publish Date	CVSS		Des	cription 8	& CVE ID		Patch	1	NCIIPC I	D
			fun app cou net and inci for is r hav par pas fun	ctionalictionalictionalictionalictionalictionalictionalictionalictionalictics	b limit the ty of the ecially control over to a port on the front poten. Once the cal access to access ty of the VE-2019	front parafted parafted parafted parafted paraftion that anel parafted the parafted					
zt420_firmw	vare				2017	10700					
N/A	20-08-2019	5	Vershi use opt pas fun app counct and ince for have par pas fun	rsions, Z pped wi er access cions. If the scode to citionali- olied, spead be se work to d the prinarray of ludes the the prinarray of etrieved we physionel of the escode to actionali-	strial Priebra priith unrest to front the option of the ecially control of the ecially control of the ecially control of the ecially control of the ecial of the ecial access to access the ecial of the	tricted of tricted of tricted of tricted of the use of the same of the partial tricker must be the partial to enter the full front partial tricker must be the full front part	N/A		0-ZEB-ZT 060919/9		
zt510_firmw	are										
N/A	20-08-2019	5			strial Pri ebra pri			N/A		0-ZEB-ZT 060919/9	
CV Scoring Scale (CVSS)	0-1 1-	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9 9-1	١0

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			shipped with unrestricted enduser access to front panel options. If the option to use a passcode to limit the functionality of the front panel is applied, specially crafted packets could be sent over the same network to a port on the printer and the printer will respond with an array of information that includes the front panel passcode for the printer. Once the passcode is retrieved, an attacker must have physical access to the front panel of the printer to enter the passcode to access the full functionality of the front panel.		
at610 firms	Vano		CVE ID : CVE-2019-10960		
zt610_firmv	vare		7 de la Ladia de la Delada de All		
N/A	20-08-2019	5	Zebra Industrial Printers All Versions, Zebra printers are shipped with unrestricted end- user access to front panel options. If the option to use a passcode to limit the functionality of the front panel is applied, specially crafted packets could be sent over the same network to a port on the printer and the printer will respond with an array of information that includes the front panel passcode for the printer. Once the passcode is retrieved, an attacker must have physical access to the front panel of the printer to enter the passcode to access the full functionality of the front panel. CVE ID: CVE-2019-10960	N/A	O-ZEB-ZT61- 060919/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
zt620_firmware					
N/A	20-08-2019	5	Zebra Industrial Printers All Versions, Zebra printers are shipped with unrestricted enduser access to front panel options. If the option to use a passcode to limit the functionality of the front panel is applied, specially crafted packets could be sent over the same network to a port on the printer and the printer will respond with an array of information that includes the front panel passcode for the printer. Once the passcode is retrieved, an attacker must have physical access to the front panel of the printer to enter the passcode to access the full functionality of the front panel. CVE ID: CVE-2019-10960	N/A	O-ZEB-ZT62- 060919/960