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_studio					
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_ShowPlugInDialog+0x000000000023d060. **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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/3

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-2019-8002**		
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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/6

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 Dereference	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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8007**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/9

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/12

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-2019-8011**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8013**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/15

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-8014**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/16
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/17
NULL Pointer Dereference	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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/18

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/21

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-8020**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/22
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-2019-8022**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/23
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	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/24

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8025**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/27

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8028**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/29
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/30

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8029**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/31
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-2019-8031**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/32
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/33

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**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/36

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

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, 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-2019-8036**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8038**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/40
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/41
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	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/42

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/45

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8044**		
NULL Pointer Dereference	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-2019-8045**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/46
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-2019-8046**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/47
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/48

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-2019-8047**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/49
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/50
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	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/51

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have a 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8052**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/54

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8053**		
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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8055**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8056**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/60

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-8059**		
Improper Neutralization 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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/61
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-2019-8061**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/62
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/63

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-2019-8077**		
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/64
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/65
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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/66

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/68
Integer Overflow or Wraparound	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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/69

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 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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/70
Integer Overflow or Wraparound	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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/72

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		5	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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/75

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-2019-8105**		
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, 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-2019-8106**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/76
acrobat_reader_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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/78

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/81

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Dereference	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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8007**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/84

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/87

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8013**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/90

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/92
NULL Pointer Dereference	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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/93

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/96

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8022**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/99

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8025**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/102

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8028**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/105

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/108

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/111

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, 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, 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-2019-8036**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/114

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/117

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/120

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 Dereference	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-2019-8045**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8046**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/123

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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/126

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8052**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/129

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8055**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/132

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/135

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 Neutralization 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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, 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-2019-8061**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/138

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/143
Integer Overflow or Wraparound	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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/144

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/145
Integer Overflow or Wraparound	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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/147

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, 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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-41.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://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060919/150

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, and 2015.006.30498 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-8105**	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-2019-8106**	https://helpx.adobe.com/security/products/acrobat/apsb19-41.html	A-ADO-ACRO-060919/151
creative_cloud					
N/A	16-08-2019	5	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://helpx.adobe.com/security/products/creative-cloud/apsb19-39.html	A-ADO-CREA-060919/152
N/A	16-08-2019	10	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://helpx.adobe.com/security/products/creative-cloud/apsb19-39.html	A-ADO-CREA-060919/153
Improper	16-08-2019	10	Creative Cloud Desktop	https://h	A-ADO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			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**	elpx.adobe.com/security/products/creative-cloud/apsb19-39.html	CREA-060919/154
Information Exposure	16-08-2019	5	Creative Cloud Desktop Application 4.6.1 and earlier versions have an insecure transmission of sensitive data vulnerability. Successful exploitation could lead to information leakage. **CVE ID : CVE-2019-8063**	https://helpx.adobe.com/security/products/creative-cloud/apsb19-39.html	A-ADO-CREA-060919/155
photoshop_cc					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-08-2019	10	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**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/156
Incorrect Type Conversion or Cast	26-08-2019	10	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-2019-7969**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/157
Incorrect Type Conversion or Cast	26-08-2019	10	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://helpx.adobe.com/security/products/pho	A-ADO-PHOT-060919/158

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
			arbitrary code execution. **CVE ID : CVE-2019-7970**	toshop/apsb19-44.html	
Incorrect Type Conversion or Cast	26-08-2019	10	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-2019-7971**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/159
Incorrect Type Conversion or Cast	26-08-2019	10	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-2019-7972**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/160
Incorrect Type Conversion or Cast	26-08-2019	10	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**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/161
Incorrect Type Conversion or Cast	26-08-2019	10	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-2019-7974**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/162
Incorrect Type Conversion or Cast	26-08-2019	10	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://helpx.adobe.com/security/products/pho	A-ADO-PHOT-060919/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-7975**	toshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/pho	A-ADO-PHOT-060919/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-7980**	toshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.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://helpx.adobe.com/security/products/pho	A-ADO-PHOT-060919/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			arbitrary code execution. **CVE ID : CVE-2019-7985**	toshop/apsb19-44.html	
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-2019-7986**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/174
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-2019-7987**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/175
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://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/176
Improper Neutralization 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-ADO-PHOT-060919/177
Improper Restriction of Operations	26-08-2019	10	Adobe Photoshop CC versions 19.1.8 and earlier and 20.0.5 and earlier have a heap overflow vulnerability. Successful	https://helpx.adobe.com/security/pro	A-ADO-PHOT-060919/178

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
within the Bounds of a Memory Buffer			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7990**	ducts/photoshop/apsb19-44.html	
Out-of-bounds Read	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 read vulnerability. Successful exploitation could lead to memory leak. **CVE ID : CVE-2019-7991**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/179
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-2019-7992**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/180
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-08-2019	10	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://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/181
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-2019-7994**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/182
Out-of-bounds Read	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 read vulnerability. Successful	https://helpx.adobe.com/security/pro	A-ADO-PHOT-060919/183

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
			exploitation could lead to memory leak. **CVE ID : CVE-2019-7995**	ducts/photoshop/apsb19-44.html	
Out-of-bounds Read	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 read vulnerability. Successful exploitation could lead to memory leak. **CVE ID : CVE-2019-7996**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/184
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-2019-7997**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/185
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-2019-7998**	https://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/186
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://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/187
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://helpx.adobe.com/security/pro	A-ADO-PHOT-060919/188

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
			exploitation could lead to memory leak. **CVE ID : CVE-2019-8000**	ducts/photoshop/apsb19-44.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://helpx.adobe.com/security/products/photoshop/apsb19-44.html	A-ADO-PHOT-060919/189
experience_manager					
Improper Authentication	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://helpx.adobe.com/security/products/experience-manager/apsb19-42.html	A-ADO-EXPE-060919/190
adplug_project					
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 Neutralization 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	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Alkacon					
opencms_apollo_template					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-08-2019	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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-08-2019	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
Information Exposure	27-08-2019	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
opencms					
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-08-2019	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
altavoz					
prontuscms					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-08-2019	10	cgi-cpn/xcoding/prontus_videocut.cgi 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 Neutralization 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 Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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_beanutils					
Deserialization 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-APA-COMM-060919/200
Artica					
integria_ims					
Unrestricted 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	A-ART-INTE-060919/201
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	A-ASP-ASPO-060919/202

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5032		
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.words					
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://snyk.io/vuln/SNYK-JS-ASSIGNDEEP-450211	A-ASS-ASSI-060919/205
Atlassian					

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
jira					
Improper Neutralization 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	A-ATL-JIRA-060919/206
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	A-ATL-JIRA-060919/207
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	A-ATL-JIRA-060919/208
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	A-ATL-JIRA-060919/209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11587		
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 Neutralization 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

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	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_plugin_manager					
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					
freeware_advanced_audio_decoder_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

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
			negative, a buffer overflow is later performed via getdword_n(&ld->start[words], ld->bytes_left). **CVE ID : CVE-2019-15296**		
Autodesk					
design_review					
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://www.autodesk.com/trust/security-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://www.autodesk.com/trust/security-advisories/adsk-sa-2019-0002	A-AUT-DESI-060919/219
Bedita					
bedita					
Improper Neutralization 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

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
belwith-keeler					
hickory_smart					
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HickorySmartLog/Logs/SRDeviceLog.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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-08-2019	6.8	components/Modals/HelpModal.jsx 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	A-BLO-BLOO-060919/224
Bolt					
bolt					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	Bolt before 3.6.10 has XSS via a title that is mishandled in the system log. **CVE ID : CVE-2019-15483**	N/A	A-BOL-BOLT-060919/225
Improper Neutralization of Input	23-08-2019	4.3	Bolt before 3.6.10 has XSS via an image's alt or title field. **CVE ID : CVE-2019-15484**	N/A	A-BOL-BOLT-060919/226

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 Neutralization 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/FilesystemManager.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-webpanel					
centos_web_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-08-2019	3.5	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

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
			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	A-CEN-CENT-060919/231
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	A-CEN-CENT-060919/232
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. **CVE ID : CVE-2019-14246**	N/A	A-CEN-CENT-060919/233
Cisco					
unified_contact_center_express					
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	A-CIS-UNIF-060919/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Improper Input Validation	21-08-2019	9	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 Authentication	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

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 Authentication	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 Authentication	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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, 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	A-CIS-UCS_-060919/240
ucs_director_express_for_big_data					
Use of Hard-coded Credentials	21-08-2019	10	A vulnerability in Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS	N/A	A-CIS-UCS_-060919/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Input Validation	21-08-2019	9	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	N/A	A-CIS-UCS_-060919/242

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
			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 Authentication	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 Authentication	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	1-2	2-3	3-4	4-5	5-6	6-7	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 Authentication	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	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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_computing_system					
Improper Input Validation	21-08-2019	9	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	A-CIS-UNIF-060919/247
Improper Authorization	21-08-2019	6.5	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to	N/A	A-CIS-UNIF-060919/248

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 Neutralization 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

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
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 Authorization	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	A-CIS-UNIF-060919/251
Improper Neutralization 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	A-CIS-UNIF-060919/252

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
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 Neutralization 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 user-supplied 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, system-level commands with root privileges on an affected device. **CVE ID : CVE-2019-1865**	N/A	A-CIS-UNIF-060919/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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	A-CIS-UNIF-060919/254
Improper Neutralization 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	A-CIS-UNIF-060919/255

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 Neutralization 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 user-supplied 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 Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow an attacker with administrator privileges to execute arbitrary commands on the device with full root privileges. **CVE ID : CVE-2019-1896**		
NULL Pointer Dereference	21-08-2019	7.8	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to cause the web server process to crash, causing a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient validation of user-supplied input on the web interface. An attacker could exploit this vulnerability by submitting a crafted HTTP request to certain endpoints of the affected software. A successful exploit could allow an attacker to cause the web server to crash. Physical access to the device may be required for a restart. **CVE ID : CVE-2019-1900**	N/A	A-CIS-UNIF-060919/258
firepower_threat_defense					
Improper Access Control	21-08-2019	5	A vulnerability in the application policy configuration of the Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data. The vulnerability is due to insufficient application identification. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A	N/A	A-CIS-FIRE-060919/259

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain unauthorized read access to sensitive data. **CVE ID : CVE-2019-12627**		
integrated_management_controller_supervisor					
Improper Authorization	21-08-2019	6.5	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to 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**	N/A	A-CIS-INTE-060919/260
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	N/A	A-CIS-INTE-060919/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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**		
Improper Input Validation	21-08-2019	9	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-INTE-060919/262
Improper Authentication	21-08-2019	10	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Supervisor,	N/A	A-CIS-INTE-060919/263

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://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_security_advisories/Users_can_restore_files_to_locations_they_do_not_have_write_access_to	A-COD-CODE-060919/264

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
crashplan_for_small_business					
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://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_security_advisories/Users_can_restore_files_to_locations_they_do_not_have_write_access_to	A-COD-CRAS-060919/265
Codection					
import_users_from_csv_with_meta					
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 Neutralization 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

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
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-08-2019	4.3	The import-users-from-csv-with-meta plugin before 1.14.0.3 for WordPress has XSS. **CVE ID : CVE-2019-15328**	N/A	A-COD-IMPO-060919/268
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 CSRF. **CVE ID : CVE-2019-15329**	N/A	A-COD-IMPO-060919/269
comelz					
quark					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-08-2019	5	comelz Quark before 2019-03-26 allows directory traversal to locations outside of the project directory. **CVE ID : CVE-2019-15520**	N/A	A-COM-QUAR-060919/270
compassionuk					
compassion_switzerland					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-08-2019	7.5	The Compassion Switzerland addons 10.01.4 for Odoo allow SQL injection in models/partner_compassion.py. **CVE ID : CVE-2019-15564**	N/A	A-COM-COMP-060919/271
cszcms					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
csz_cms					
Unrestricted 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_project					
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
Uncontrolled Resource Consumption	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

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
Uncontrolled Resource Consumption	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**	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_context 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					
domoticz					
Improper Neutralization 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
easyupdatesmanager					
easy_updates_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	2-3	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**		
elearningfreak					
insert_or_embed_articulate_content					
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
Unrestricted 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 Neutralization 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					

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
envoy					
Uncontrolled Resource Consumption	19-08-2019	5	In Envoy through 1.11.1, users may configure a route to match incoming path headers via the libstdc++ regular expression implementation. A remote attacker may send a request with a very long URI to result in a denial of service (memory consumption). This is a related issue to CVE-2019-14993. **CVE ID : CVE-2019-15225**	N/A	A-ENV-ENVO-060919/284
eprosima					
fast-rtps					
N/A	18-08-2019	5	The Access Control plugin in eProsima Fast RTPS through 1.9.0 does not check partition permissions from remote participant connections, which can lead to policy bypass for a secure Data Distribution Service (DDS) partition. **CVE ID : CVE-2019-15136**	N/A	A-EPR-FAST-060919/285
Improper Access Control	18-08-2019	5	The Access Control plugin in eProsima Fast RTPS through 1.9.0 allows fnmatch pattern matches with topic name strings (instead of the permission expressions themselves), which can lead to unintended connections between participants in a Data Distribution Service (DDS) network. **CVE ID : CVE-2019-15137**	N/A	A-EPR-FAST-060919/286
etoilewebdesign					
ultimate_faq					
Improper Neutralizati	27-08-2019	4.3	The ultimate-faqs plugin before	N/A	A-ETO-ULTI-

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
on of Input During Web Page Generation ('Cross-site Scripting')			1.8.22 for WordPress has XSS. **CVE ID : CVE-2019-15643**		060919/287
extenua					
silvershield					
N/A	17-08-2019	7.2	extenua SilverSHielD 6.x fails to secure its ProgramData folder, leading to a Local Privilege Escalation to SYSTEM. The attacker must replace SilverShield.config.sqlite with a version containing an additional user account, and then use SSH and port forwarding to reach a 127.0.0.1 service. **CVE ID : CVE-2019-13069**	N/A	A-EXT-SILV-060919/288
Eyesofnetwork					
eyesofnetwork					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-08-2019	6.5	EyesOfNetwork 5.1 allows Remote Command Execution via shell metacharacters in the module/tool_all/ host field. **CVE ID : CVE-2019-14923**	N/A	A-EYE-EYES-060919/289
Facebook					
fizz					
Uncontrolled Resource Consumption	20-08-2019	7.8	A peer could send empty handshake fragments containing only padding which would be kept in memory until a full handshake was received, resulting in memory exhaustion.	https://www.facebook.com/security/advisories/cve-2019-	A-FAC-FIZZ-060919/290

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. **CVE ID : CVE-2019-11924**	11924	
forcepoint					
next_generation_firewall					
Improper Authentication	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://support.forcepoint.com/KBArticle?id=000017474	A-FOR-NEXT-060919/291
former_project					
former					
Improper Neutralization 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	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fortiguard					
fortios_ips_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://fortiguard.com/advisory/FG-IR-19-145	A-FOR-FORT-060919/293
Fortinet					
fortinac					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	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. **CVE ID : CVE-2019-5594**	https://fortiguard.com/advisory/FG-IR-19-140	A-FOR-FORT-060919/294
gchq					
cyberchef					
Improper Neutralization of Input During Web Page	26-08-2019	4.3	CyberChef before 8.31.2 allows XSS in core/operations/TextEncodingBruteForce.mjs.	N/A	A-GCH-CYBE-060919/295

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')			**CVE ID : CVE-2019-15532**		
Genetechsolutions					
pie_register					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-08-2019	7.5	The pie-register plugin before 3.1.2 for WordPress has SQL injection, a different issue than CVE-2018-10969. **CVE ID : CVE-2019-15659**	N/A	A-GEN-PIE_-060919/296
getflightpath					
flightpath					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	4.3	FlightPath 4.8.3 has XSS in the Content, Edit urgent message, and Users sections of the Admin Console. This could lead to cookie stealing and other malicious actions. **CVE ID : CVE-2019-15227**	N/A	A-GET-FLIG-060919/297
giflib_project					
giflib					
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	A-GIF-GIFL-060919/298
GNU					
libextractor					

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
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					
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 Neutralization 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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	27-08-2019	6.5	The groundhogg plugin before 1.3.5 for WordPress has wp-admin/admin-ajax.php?action=bulk_action_listener remote code execution. **CVE ID : CVE-2019-15647**	N/A	A-GRO-GROU-060919/304
hackmd					
codimd					
Improper Neutralization 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	A-HAC-CODI-060919/305
httpie					
httpie					
URL Redirection to Untrusted Site ('Open Redirect')	23-08-2019	5.8	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. **CVE ID : CVE-2019-10751**	N/A	A-HTT-HTTP-060919/306
humanica					
humatrix_7					
Information Exposure	18-08-2019	5	The Recruitment module in Humanica Humatrix 7 1.0.0.203 and 1.0.0.681 allows an unauthenticated attacker to access all candidates' files in the photo folder on the website by specifying a "user id" parameter	N/A	A-HUM-HUMA-060919/307

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**		
Unrestricted 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_appliance					
Improper Neutralization 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://www.ibm.com/support/docview.wss?uid=ibm10958933	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	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			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_dynamic_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. **CVE ID : CVE-2019-4253**	N/A	A-IBM-INFO-060919/311
datapower_gateway					
Improper Neutralization 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://www.ibm.com/support/docview.wss?uid=ibm10958933	A-IBM-DATA-060919/312
emptoris_sourcing					
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://www.ibm.com/support/docview.wss?uid=ibm10880221	A-IBM-EMPT-060919/313

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
			ID: 161034. **CVE ID : CVE-2019-4308**		
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: 164068. **CVE ID : CVE-2019-4484**	https://www.ibm.com/support/docview.wss?uid=ibm10880221	A-IBM-EMPT-060919/314
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. **CVE ID : CVE-2019-4485**	https://www.ibm.com/support/docview.wss?uid=ibm10880221	A-IBM-EMPT-060919/315
emptoris_spend_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. **CVE ID : CVE-2019-4308**	https://www.ibm.com/support/docview.wss?uid=ibm10880221	A-IBM-EMPT-060919/316
Improper Neutralization of	20-08-2019	7.5	IBM Contract Management 10.1.0 through 10.1.3 and IBM Emptoris Spend Analysis 10.1.0 through	https://www.ibm.com/supp	A-IBM-EMPT-060919/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			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 back-end database. IBM X-Force ID: 164064. **CVE ID : CVE-2019-4481**	ort/docview.wss?uid=ibm10880223	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	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://www.ibm.com/support/docview.wss?uid=ibm10880217	A-IBM-EMPT-060919/318
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	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 back-end database. IBM X-Force ID: 164067. **CVE ID : CVE-2019-4483**	https://www.ibm.com/support/docview.wss?uid=ibm10880223	A-IBM-EMPT-060919/319
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	https://www.ibm.com/support/docview.wss?uid=ibm10880221	A-IBM-EMPT-060919/320

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. **CVE ID : CVE-2019-4485**	https://www.ibm.com/support/docview.wss?uid=ibm10880221	A-IBM-EMPT-060919/321
security_guardium_big_data_intelligence					
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://www.ibm.com/support/docview.wss?uid=ibm10960298	A-IBM-SECU-060919/322
Uncontrolled Resource Consumption	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://www.ibm.com/support/docview.wss?uid=ibm10960858	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://www.ibm.com/support/docvi	A-IBM-SECU-060919/324

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. **CVE ID : CVE-2019-4340**	ew.wss?uid=ibm10960856	
infosphere_global_name_management					
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**	https://www.ibm.com/support/docview.wss?uid=ibm10958081	A-IBM-INFO-060919/325
infosphere_identity_insight					
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**	https://www.ibm.com/support/docview.wss?uid=ibm10958081	A-IBM-INFO-060919/326
security_access_manager_for_enterprise_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	N/A	A-IBM-SECU-060919/327

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
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					
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://www.ibm.com/support/docview.wss?uid=ibm10958193	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. **CVE ID : CVE-2019-4437**	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://www.ibm.com/support/docview.wss?uid=ibm10960848	A-IBM-API_-060919/330
intelligent_operations_center					
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://www.ibm.com/support/docvi	A-IBM-INTE-060919/331

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. **CVE ID : CVE-2019-4419**	ew.wss?uid=ibm10956433	
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://www.ibm.com/support/docview.wss?uid=ibm10956429	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. **CVE ID : CVE-2019-4419**	https://www.ibm.com/support/docview.wss?uid=ibm10956433	A-IBM-INTE-060919/333
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://www.ibm.com/support/docview.wss?uid=ibm10956429	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://www.ibm.c	A-IBM-WATE-

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/support/docview.wss?uid=ibm10956433	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://www.ibm.com/support/docview.wss?uid=ibm10956429	A-IBM-WATE-060919/336
business_automation_workflow					
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. **CVE ID : CVE-2019-4424**	https://www.ibm.com/support/docview.wss?uid=ibm10959537	A-IBM-BUSI-060919/337
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://www.ibm.com/support/docview.wss?uid=ibm10959261	A-IBM-BUSI-060919/338

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4425		
business_process_manager					
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. **CVE ID : CVE-2019-4424**	https://www.ibm.com/support/docview.wss?uid=ibm10959537	A-IBM-BUSI-060919/339
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. **CVE ID : CVE-2019-4425**	https://www.ibm.com/support/docview.wss?uid=ibm10959261	A-IBM-BUSI-060919/340
cloud_private					
Cross-Site Request Forgery (CSRF)	20-08-2019	6.8	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	A-IBM-CLOU-060919/341
Improper Neutralization of Input During Web Page Generation	20-08-2019	3.5	IBM Cloud Private 3.1.1 and 3.1.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	N/A	A-IBM-CLOU-060919/342

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
('Cross-site Scripting')			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158146. **CVE ID : CVE-2019-4120**		
Igniterealtime					
openfire					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	Ignite Realtime Openfire before 4.4.1 has reflected XSS via an LDAP setup test. **CVE ID : CVE-2019-15488**	N/A	A-IGN-OPEN-060919/343
imagely					
nextgen_gallery					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-08-2019	7.5	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-IMA-NEXT-060919/344
Imagemagick					
imagemagick					
Out-of-bounds Read	18-08-2019	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-IMA-IMAG-060919/345

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
			Read) in ReadXWDImage in coders/xwd.c by crafting a corrupted XWD image file, a different vulnerability than CVE-2019-11472. **CVE ID : CVE-2019-15139**		
Use After Free	18-08-2019	6.8	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**	N/A	A-IMA-IMAG-060919/346
Out-of-bounds Read	18-08-2019	4.3	WriteTIFFImage in coders/tiff.c in ImageMagick 7.0.8-43 Q16 allows attackers to cause a denial-of-service (application crash resulting from a heap-based buffer over-read) via a crafted TIFF image file, related to TIFFRewriteDirectory, TIFFWriteDirectory, TIFFWriteDirectorySec, and TIFFWriteDirectoryTagColormap in tif_dirwrite.c of LibTIFF. NOTE: this occurs because of an incomplete fix for CVE-2019-11597. **CVE ID : CVE-2019-15141**	N/A	A-IMA-IMAG-060919/347
impress					
givewp					
Improper Neutralization 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**	N/A	A-IMP-GIVE-060919/348

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')					
instamojo					
payment_gateway					
Improper Input Validation	29-08-2019	5	card/pay/.../amount in the WooCommerce Instamojo Payment Gateway plugin 1.0.7 for WordPress allows Parameter Tampering in the sign parameter, as demonstrated by purchasing an item for lower than the intended price. **CVE ID : CVE-2019-14977**	N/A	A-INS-PAYM-060919/349
Intel					
authenticate					
N/A	19-08-2019	4.6	Improper permissions in the software installer for Intel(R) Authenticate before 3.8 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-11143**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00275.html	A-INT-AUTH-060919/350
remote_displays_sdk					
N/A	19-08-2019	4.6	Improper permissions in the installer for Intel(R) Remote Displays SDK before version 2.0.1 R2 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-11148**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00277.ht	A-INT-REMO-060919/351

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
				ml	
processor_identification_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://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00281.html	A-INT-PROC-060919/352
raid_web_console_2					
Improper Authentication	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://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00246.html	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	2-3	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	28-08-2019	6.5	A sandbox bypass vulnerability in Jenkins Splunk Plugin 1.7.4 and earlier allowed attackers with Overall/Read permission to provide a Groovy script to an HTTP endpoint that can result in arbitrary code execution on the Jenkins master JVM. **CVE ID : CVE-2019-10390**	N/A	A-JEN-SPLU-060919/355
jooby					
jooby					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-08-2019	4.3	Jooby before 1.6.4 has XSS via the default error handler. **CVE ID : CVE-2019-15477**	N/A	A-JOO-JOOB-060919/356
Kaseya					
virtual_system_administrator					
Information Exposure	26-08-2019	7.8	An issue was discovered in Kaseya Virtual System Administrator (VSA) through 9.4.0.37. It has a critical information disclosure vulnerability. An unauthenticated attacker can send properly formatted requests to the web application and download sensitive files and information. For example, the /DATAREPORTS directory can be farmed for reports. Because this directory contains the results of reports such as NMAP, Patch Status, and Active Directory domain metadata, an attacker can easily collect this critical information	N/A	A-KAS-VIRT-060919/357

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 Neutralization 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 Neutralization 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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
laracom					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-08-2019	4.3	laracom (aka Laravel FREE E-Commerce Software) 1.4.11 has search?q= XSS. **CVE ID : CVE-2019-15489**	N/A	A-LAR-LARA-060919/361
Lenovo					
solution_center					
Information Exposure	21-08-2019	7.5	A vulnerability reported in Lenovo Solution Center version 03.12.003, which is no longer supported, could allow log files to be written to non-standard locations, potentially leading to privilege escalation. Lenovo ended support for Lenovo Solution Center and recommended that customers migrate to Lenovo Vantage or Lenovo Diagnostics in April 2018. **CVE ID : CVE-2019-6177**	https://support.lenovo.com/solutions/LEN-27811	A-LEN-SOLU-060919/362
librenms					
librenms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-08-2019	3.5	LibreNMS v1.54 has XSS in the Create User, Inventory, Add Device, Notifications, Alert Rule, Create Maintenance, and Alert Template sections of the admin console. This could lead to cookie stealing and other malicious actions. This vulnerability can be exploited with an authenticated account. **CVE ID : CVE-2019-15230**	N/A	A-LIB-LIBR-060919/363
Live555					

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
streaming_media					
Use After Free	19-08-2019	7.5	Live555 before 2019.08.16 has a Use-After-Free because GenericMediaServer::createNewClientSessionWithId can generate the same client session ID in succession, which is mishandled by the MPEG1or2 and Matroska file demultiplexors. **CVE ID : CVE-2019-15232**	N/A	A-LIV-STRE-060919/364
Lsoft					
listserv					
Improper Neutralization 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	A-LSO-LIST-060919/365
manageyourteam					
myt_project_management					
Cross-Site Request Forgery (CSRF)	28-08-2019	6.8	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**	N/A	A-MAN-MYT_-060919/366
Mcafee					
data_loss_prevention_endpoint					
Improper Restriction of Operations	21-08-2019	4.9	Buffer overflow in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.2.8 allows local user to cause the	https://kc.mcafee.com/corporate/index	A-MCA-DATA-060919/367

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
within the Bounds of a Memory Buffer			Windows operating system to "blue screen" via a carefully constructed message sent to DLPe which bypasses DLPe internal checks and results in DLPe reading unallocated memory. **CVE ID : CVE-2019-3633**	?page=content&id=SB10295	
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-08-2019	4.9	Buffer overflow in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.2.8 allows local user to cause the Windows operating system to "blue screen" via an encrypted message sent to DLPe which when decrypted results in DLPe reading unallocated memory. **CVE ID : CVE-2019-3634**	https://kc.mcafee.com/corporate/index?page=content&id=SB10295	A-MCA-DATA-060919/368
Microfocus					
verastream_host_integrato					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-08-2019	5	Path traversal vulnerability in Micro Focus Verastream Host Integrator (VHI), versions 7.7 SP2 and earlier, The vulnerability allows remote unauthenticated attackers to read arbitrary files. **CVE ID : CVE-2019-11654**	https://support.microfocus.com/kb/doc.php?id=7024061	A-MIC-VERA-060919/369
content_manager					
Information Exposure	30-08-2019	4	Information exposure in Micro Focus Content Manager, versions 9.1, 9.2 and 9.3. This vulnerability when configured to use an Oracle database, allows valid system users to gain access to a limited subset of records they would not normally be able to access when the system is in an undisclosed	https://softwaresupport.softwaregrp.com/doc/KM03496282	A-MIC-CONT-060919/370

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
			abnormal state. **CVE ID : CVE-2019-11658**		
micropyramid					
django_crm					
Cross-Site Request Forgery (CSRF)	27-08-2019	6.8	Multiple CSRF issues exist in MicroPyramid Django CRM 0.2.1 via /change-password-by-admin/, /api/settings/add/, /cases/create/, /change-password-by-admin/, /comment/add/, /documents/1/view/, /documents/create/, /opportunities/create/, and /login/. **CVE ID : CVE-2019-11457**	N/A	A-MIC-DJAN-060919/371
mirasys					
mirasys_vms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-08-2019	5	Mirasys VMS before V7.6.1 and 8.x before V8.3.2 mishandles the Download() method of AutoUpdateService in SMServer.exe, leading to Directory Traversal. An attacker could use ..\ with this method to iterate over lists of interesting system files and download them without previous authentication. This includes SAM-database backups, Web.config files, etc. and might cause a serious impact on confidentiality. **CVE ID : CVE-2019-11029**	N/A	A-MIR-MIRA-060919/372
Deserialization of Untrusted Data	22-08-2019	10	Mirasys VMS before V7.6.1 and 8.x before V8.3.2 mishandles the Mirasys.Common.Utils.Security.DataCrypt method in Common.dll in AuditTrailService in	N/A	A-MIR-MIRA-060919/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMServer.exe. This method triggers insecure deserialization within the .NET garbage collector, in which a gadget (contained in a serialized object) may be executed with SYSTEM privileges. The attacker must properly encrypt the object; however, the hardcoded keys are available. **CVE ID : CVE-2019-11030**		
Unrestricted Upload of File with Dangerous Type	22-08-2019	10	Mirasys VMS before V7.6.1 and 8.x before V8.3.2 mishandles the auto-update feature of IDVRUpdateService2 in DVRServer.exe. An attacker can upload files with a Setup-Files action, and then execute these files with SYSTEM privileges. **CVE ID : CVE-2019-11031**	N/A	A-MIR-MIRA-060919/374
mixin-deep_project					
mixin-deep					
Argument Injection or Modification	23-08-2019	7.5	mixin-deep is vulnerable to Prototype Pollution in versions before 1.3.2 and version 2.0.0. The function mixin-deep could be tricked into adding or modifying properties of Object.prototype using a constructor payload. **CVE ID : CVE-2019-10746**	N/A	A-MIX-MIXI-060919/375
my_calendar_project					
my_calendar					
Improper Neutralization of Input During Web Page Generation ('Cross-site	28-08-2019	4.3	The my-calendar plugin before 3.1.10 for WordPress has XSS. **CVE ID : CVE-2019-15713**	N/A	A-MY_-MY_C-060919/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Ncrafts					
formcraft					
Cross-Site Request Forgery (CSRF)	16-08-2019	6.8	The formcraft-form-builder plugin before 1.2.2 for WordPress has CSRF. **CVE ID : CVE-2019-15114**	N/A	A-NCR-FORM-060919/377
ncurses_project					
ncurses					
Use of Externally-Controlled Format String	26-08-2019	6.4	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/A	A-NCU-NCUR-060919/378
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-08-2019	7.5	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	A-NCU-NCUR-060919/379
networkgenomics					
mitogen					
N/A	18-08-2019	6.8	** 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	A-NET-MITO-060919/380

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_project					
nokogiri					
Improper Neutralization 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_file` 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

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5477		
nps_project					
nps					
N/A	16-08-2019	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-NPS-060919/383
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. **CVE ID : CVE-2019-13013**	N/A	A-OBD-LITT-060919/384
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-LITT-060919/385
octopus					
server					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure Through Log Files	23-08-2019	3.5	In Octopus Deploy versions 2018.8.4 to 2019.7.6, when a web request proxy is configured, an authenticated user (in certain limited special-characters circumstances) could trigger a deployment that writes the web request proxy password to the deployment log in cleartext. This is fixed in 2019.7.7. The fix was back-ported to LTS 2019.6.7 as well as LTS 2019.3.8. **CVE ID : CVE-2019-15507**	N/A	A-OCT-SERV-060919/386
Information Exposure Through Log Files	23-08-2019	3.5	In Octopus Tentacle versions 3.0.8 to 5.0.0, when a web request proxy is configured, an authenticated user (in certain limited OctopusPrintVariables circumstances) could trigger a deployment that writes the web request proxy password to the deployment log in cleartext. This is fixed in 5.0.1. The fix was back-ported to 4.0.7. **CVE ID : CVE-2019-15508**	N/A	A-OCT-SERV-060919/387
octopus_deploy					
Information Exposure	27-08-2019	4	In Octopus Deploy 2019.7.3 through 2019.7.9, in certain circumstances, an authenticated user with VariableView permissions could view sensitive values. This is fixed in 2019.7.10. **CVE ID : CVE-2019-15698**	N/A	A-OCT-OCTO-060919/388
ohdsi					
webapi					
Improper Neutralization of	26-08-2019	7.5	Observational Health Data Sciences and Informatics (OHDSI) WebAPI before 2.7.2 allows SQL	N/A	A-OHD-WEBA-060919/389

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
Special Elements used in an SQL Command ('SQL Injection')			injection in FeatureExtractionService.java. **CVE ID : CVE-2019-15563**		
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_-060919/390
Open-emr					
openemr					
Improper Neutralization 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-060919/391
Improper Neutralization 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-060919/392

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')			arbitrary code in the context of a user's session. **CVE ID : CVE-2019-3964**		
Improper Neutralization 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 Neutralization 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 Neutralization 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	NCIIPC ID
openpgpjs					
Improper Verification of Cryptographic 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-OPE-OPEN-060919/397
Improper Verification of Cryptographic 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-OPE-OPEN-060919/398
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-OPE-OPEN-060919/399
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-tlv 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-OPE-OPEN-060919/400

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 Wraparound	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

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
Open-xchange					
open-xchange_appsuite					
Improper Input Validation	20-08-2019	5.8	OX App Suite 7.10.1 allows Content Spoofing. **CVE ID : CVE-2019-11521**	N/A	A-OPE-OPEN-060919/404
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	3.5	OX App Suite 7.10.0 to 7.10.2 allows XSS. **CVE ID : CVE-2019-11522**	N/A	A-OPE-OPEN-060919/405
N/A	20-08-2019	2.1	OX App Suite 7.10.1 and earlier has Insecure Permissions. **CVE ID : CVE-2019-11806**	N/A	A-OPE-OPEN-060919/406
optiontree_project					
optiontree					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-08-2019	7.5	The option-tree plugin before 2.7.0 for WordPress has Object Injection by leveraging a valid nonce. **CVE ID : CVE-2019-15319**	N/A	A-OPT-OPTI-060919/407
Improper Neutralization of Special Elements in Output Used by a Downstream	22-08-2019	7.5	The option-tree plugin before 2.7.3 for WordPress has Object Injection because the + character is mishandled. **CVE ID : CVE-2019-15320**	N/A	A-OPT-OPTI-060919/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-08-2019	7.5	The option-tree plugin before 2.7.3 for WordPress has Object Injection because serialized classes are mishandled. **CVE ID : CVE-2019-15321**	N/A	A-OPT-OPTI-060919/409
Otrs					
otrs					
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 might unknowingly disclose their session ID by sharing the link of an embedded ticket article with third parties. This identifier can be then be potentially abused in order to impersonate the agent user. **CVE ID : CVE-2019-12746**	N/A	A-OTR-OTRS-060919/410
N/A	21-08-2019	4	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.8, and Community Edition 5.0.x through 5.0.36 and 6.0.x through 6.0.19. An attacker who is logged into OTRS as an agent user with appropriate permissions can leverage OTRS notification tags in templates in order to disclose hashed user passwords.	N/A	A-OTR-OTRS-060919/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13458		
Paloaltonetworks					
twistlock					
N/A	23-08-2019	6	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. **CVE ID : CVE-2019-1583**	https://securityadvisories.paloaltonetworks.com/home/detail/162	A-PAL-TWIS-060919/412
pancurses_project					
pancurses					
Use of Externally-Controlled Format String	26-08-2019	6.4	An issue was discovered in the pancurses crate through 0.16.1 for Rust. printw and mvprintw have format string vulnerabilities. **CVE ID : CVE-2019-15546**	N/A	A-PAN-PANC-060919/413
pivotal_software					
application_service					
Improper Access Control	19-08-2019	4.1	Pivotal Apps Manager, included in Pivotal Application Service versions 2.3.x prior to 2.3.16, 2.4.x prior to 2.4.12, 2.5.x prior to 2.5.8, and 2.6.x prior to 2.6.3, makes a request to the /cloudapplication endpoint via Spring actuator, and subsequent requests via unsecured http. An adjacent unauthenticated user could eavesdrop on the network traffic and gain access to the unencrypted token allowing the attacker to read the type of access	https://pivotal.io/security/cve-2019-11276	A-PIV-APPL-060919/414

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
			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-module-builder_project					
raml-module-builder					
Improper Neutralization 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://help.rapid7.com/nexpose/en-us/release-notes/archive/2019/02/	A-RAP-NEXP-060919/416
insightappsec					

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://help.rapid7.com/insightappsec/release-notes/archive/2019/07/	A-RAP-INSI-060919/417
riot-os					
riot					
Uncontrolled Resource Consumption	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/tcp/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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
desktop_password_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.games					
mw-oauth2client					
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-guard					
search_guard					
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	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative user is able to retrieve bcrypt password hashes of other users configured in the internal user database. **CVE ID : CVE-2019-13421**		
URL Redirection to Untrusted Site ('Open Redirect')	23-08-2019	5.8	Search Guard Kibana Plugin versions before 5.6.8-7 and before 6.x.y-12 had an issue that an attacker can redirect the user to a potentially malicious site upon Kibana login. **CVE ID : CVE-2019-13422**	N/A	A-SEA-SEAR-060919/423
N/A	23-08-2019	6.5	Search Guard Kibana Plugin versions before 5.6.8-7 and before 6.x.y-12 had an issue that an authenticated Kibana user could impersonate as kibanaserver user when providing wrong credentials when all of the following conditions a-c are true: a) Kibana is configured to use Single-Sign-On as authentication method, one of Kerberos, JWT, Proxy, Client certificate. b) The kibanaserver user is configured to use HTTP Basic as the authentication method. c) Search Guard is configured to use an SSO authentication domain and HTTP Basic at the same time **CVE ID : CVE-2019-13423**	N/A	A-SEA-SEAR-060919/424
Sonatype					
nexus_repository_manager					
Improper Neutralization of Input During Web Page	22-08-2019	3.5	In Nexus Repository Manager before 3.18.0, users with elevated privileges can create stored XSS. **CVE ID : CVE-2019-14469**	N/A	A-SON-NEXU-060919/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')					
sphinxsearch					
sphinx					
Missing Authentication 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-library					
spoon_library					
Deserialization 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_project					
status_board					
Improper Neutralization 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 Neutralization 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	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-SWO-SWOO-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
thedaylightstudio					
fuel_cms					
Improper Neutralization 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)	0-1	1-2	2-3	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-2019-15228		
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://www.tibco.com/support/advisories/2019/08/tibco-security-advisory-august-20-2019-tibco-ftl	A-TIB-FTL-060919/434
Tiki					
tikiwiki_cms/groupware					
Improper Neutralization 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 (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
password_manager					
Untrusted Search Path	20-08-2019	9.3	A DLL hijacking vulnerability exists in Trend Micro Password Manager 5.0 in which, if exploited, would allow an attacker to load an arbitrary unsigned DLL into the signed service's process. This process is very similar, yet not identical to CVE-2019-14687. **CVE ID : CVE-2019-14684**	N/A	A-TRE-PASS-060919/436
Untrusted Search Path	20-08-2019	6.8	A DLL hijacking vulnerability exists in Trend Micro Password Manager 5.0 in which, if exploited, would allow an attacker to load an arbitrary unsigned DLL into the signed service's process. This process is very similar, yet not identical to CVE-2019-14684. **CVE ID : CVE-2019-14687**	N/A	A-TRE-PASS-060919/437
antivirus_security_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-ANTI-060919/438
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	https://esupport.trendmicro.com/en-us/home/pages/technical-support/1123421.as	A-TRE-ANTI-060919/439

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
			elevated privileges. **CVE ID : CVE-2019-14686**	px	
internet_security_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-INTE-060919/440
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://esupport.trendmicro.com/en-us/home/pages/technical-support/1123421.aspx	A-TRE-INTE-060919/441
maximum_security_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-MAXI-060919/442
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	https://esupport.trendmicro.com/en-us/home/pages/technical-	A-TRE-MAXI-060919/443

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/1123421.aspx	
premium_security_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://esupport.trendmicro.com/en-us/home/pages/technical-support/1123421.aspx	A-TRE-PREM-060919/445
ransom_buster					
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://esupport.trendmicro.com/en-us/home/pages/technical-support/1123421.aspx	A-TRE-RANS-060919/446
Valvesoftware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
steam_client					
N/A	21-08-2019	7.2	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**	N/A	A-VAL-STEA-060919/447
N/A	21-08-2019	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. **CVE ID : CVE-2019-15316**	N/A	A-VAL-STEA-060919/448
vanderbilt					
redcap					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-08-2019	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.php. 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://www.evms.edu/research/resources_services/redcap/redcap_change_log/	A-VAN-REDC-060919/449
Improper Neutralization of Input During Web	21-08-2019	3.5	REDCap before 9.3.0 allows XSS attacks against non-administrator accounts on the Data Import Tool page via a CSV	https://www.evms.edu/research/resou	A-VAN-REDC-060919/450

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
Page Generation ('Cross-site Scripting')			data import file. **CVE ID : CVE-2019-15127**	rces_services/redcap/redcap_change_log/	
webassembly					
binaryen					
NULL Pointer Dereference	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					
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_express_project					
webp_express					
Information Exposure	22-08-2019	5	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 (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-08-2019	6	The webtoffee "WordPress Users & 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_Exporter class. **CVE ID : CVE-2019-15092**	N/A	A-WEB-IMPO-060919/454
Woocommerce					
paypal_checkout_payment_gateway					
Improper Input Validation	29-08-2019	5	cgi-bin/webscr?cmd=_cart in the WooCommerce PayPal Checkout Payment Gateway plugin 1.6.17 for WordPress allows Parameter Tampering in an amount parameter (such as amount_1), as demonstrated by purchasing an item for lower than the intended price. **CVE ID : CVE-2019-14979**	N/A	A-WOO-PAYP-060919/455
payu_india_payment_gateway					
Improper Input Validation	29-08-2019	5	/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. **CVE ID : CVE-2019-14978**	N/A	A-WOO-PAYU-060919/456
wp_front_end_profile_project					
wp_front_end_profile					
Improper Neutralizati	21-08-2019	4.3	The wp-front-end-profile plugin before 0.2.2 for WordPress has	N/A	A-WP_-WP_F-

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
on of Input During Web Page Generation ('Cross-site Scripting')			XSS. **CVE ID : CVE-2019-15110**		060919/457
N/A	21-08-2019	7.5	The wp-front-end-profile plugin before 0.2.2 for WordPress has a privilege escalation issue. **CVE ID : CVE-2019-15111**	N/A	A-WP_-WP_F-060919/458
wpmadeasy					
shortcode_factory					
Improper Input Validation	22-08-2019	7.5	The shortcode-factory plugin before 2.8 for WordPress has Local File Inclusion. **CVE ID : CVE-2019-15322**	N/A	A-WPM-SHOR-060919/459
wp-members_project					
wp-members					
Cross-Site Request Forgery (CSRF)	27-08-2019	6.8	The wp-members plugin before 3.2.8 for WordPress has CSRF. **CVE ID : CVE-2019-15660**	N/A	A-WP--WP-M-060919/460
wp-slimstat					
slimstat_analytics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-08-2019	4.3	The wp-slimstat plugin before 4.8.1 for WordPress has XSS. **CVE ID : CVE-2019-15112**	N/A	A-WP--SLIM-060919/461
wpsupportplus					
wp_support_plus_responsive_ticket_system					
Improper Neutralizati	22-08-2019	4.3	The wp-support-plus-responsive-ticket-system plugin before 9.1.2	N/A	A-WPS-WP_S-

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
on of Special Elements in Output Used by a Downstream Component ('Injection')			for WordPress has HTML injection. **CVE ID : CVE-2019-15331**		060919/462
Wso2					
api_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-08-2019	3.5	An issue was discovered in WSO2 API Manager 2.6.0 before WSO2-CARBON-PATCH-4.4.0-4457. There is XSS via a crafted filename to the file-upload feature of the event simulator component. **CVE ID : CVE-2019-15108**	N/A	A-WSO-API_-060919/463
xm-online					
Xm^online_2_-_common_utils_and_endpoints					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-08-2019	7.5	XM^online 2 Common Utils and Endpoints 0.2.1 allows SQL injection, related to Constants.java, DropSchemaResolver.java, and SchemaChangeResolver.java. **CVE ID : CVE-2019-15558**	N/A	A-XM—XM^O-060919/464
Xymon					
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 &nbsp; expansion in appfeed.c.	https://lists.xymon.com/archive/2019-July/0465	A-XYM-XYMO-060919/465

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://lists.xymon.com/archive/2019-July/046570.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 &nbsp; expansion in svcstatus.c. **CVE ID : CVE-2019-13486**	https://lists.xymon.com/archive/2019-July/046570.html	A-XYM-XYMO-060919/467
Improper Neutralization 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://lists.debian.org/debian-lts-announce/2019/08/msg00032.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://lists.xymon.com/archive/2019-July/046570.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://lists.xymon.com/archive/2019-July/0465	A-XYM-XYMO-060919/470

Weakness	Publish Date	CVSS	Description & 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	In Xymon through 4.3.28, a stack-based buffer overflow vulnerability exists in the alert acknowledgment CGI tool because of &nbsp; expansion in acknowledge.c. **CVE ID : CVE-2019-13455**	https://lists.xymon.com/archive/2019-July/046570.html	A-XYM-XYMO-060919/471
yofla					
360_product_rotation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-08-2019	4.3	The 360-product-rotation plugin before 1.4.8 for WordPress has reflected XSS. **CVE ID : CVE-2019-15082**	N/A	A-YOF-360_-060919/472
youphptube					
youphptube					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-08-2019	5	plugin/Audit/Objects/AuditTable.php in YouPHPTube through 7.2 allows SQL Injection. **CVE ID : CVE-2019-14430**	N/A	A-YOU-YOUP-060919/473
Zabbix					
Zabbix					
Information Exposure	17-08-2019	5	Zabbix through 4.4.0alpha1 allows User Enumeration. With login requests, it is possible to	N/A	A-ZAB-ZABB-060919/474

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
			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://www.coalfire.com/The-Coalfire-Blog/August-2019/Getting-more-from-a-compliance-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://www.coalfire.com/The-Coalfire-Blog/August-2019/Getting-more-from-a-compliance-test	A-ZEN-ZENO-060919/476

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
Zoho					
salesiq					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-08-2019	4.3	The zoho-salesiq plugin before 1.0.9 for WordPress has stored XSS. **CVE ID : CVE-2019-15644**	N/A	A-ZOH-SALE-060919/477
Cross-Site Request Forgery (CSRF)	27-08-2019	6.8	The zoho-salesiq plugin before 1.0.9 for WordPress has CSRF. **CVE ID : CVE-2019-15645**	N/A	A-ZOH-SALE-060919/478
Operating System					
belwith-keeler					
hickory_smart_ethernet_bridge_firmware					
Information Exposure	22-08-2019	5	A cleartext transmission of sensitive information vulnerability is present in Hickory Smart Ethernet Bridge from Belwith Products, LLC. Captured data reveals that the Hickory Smart Ethernet Bridge device communicates over the network to an MQTT broker without using encryption. This exposed the default username and password used to authenticate to the MQTT broker. This issue affects Hickory Smart Ethernet Bridge, model number H077646. The firmware does not appear to contain versioning information. **CVE ID : CVE-2019-5635**	N/A	O-BEL-HICK-060919/479
Canonical					
ubuntu_linux					

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_hx220c_edge_m5_firmware					
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_codec_c60_firmware					
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

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_hx220c_af_m5_firmware					
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_hx220c_m5_firmware					
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 & CVE ID	Patch	NCIIPC ID
hyperflex_hx240c_af_m5_firmware					
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-060919/485
hyperflex_hx240c_m5_firmware					
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-060919/486
telepresence_codec_c40_firmware					
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	N/A	O-CIS-TELE-060919/487

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
			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_codec_c90_firmware					
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

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					

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 &nbsp; expansion in appfeed.c. **CVE ID : CVE-2019-13484**	https://lists.xymon.com/archive/2019-July/046570.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://lists.xymon.com/archive/2019-July/046570.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 &nbsp; expansion in svcstatus.c. **CVE ID : CVE-2019-13486**	https://lists.xymon.com/archive/2019-July/046570.html	O-DEB-DEBI-060919/493
Deserialization 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	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			might unknowingly disclose their session ID by sharing the link of an embedded ticket article with third parties. This identifier can be then be potentially abused in order to impersonate the agent user. **CVE ID : CVE-2019-12746**		
Improper Neutralization 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://lists.debian.org/debian-lts-announce/2019/08/msg00032.html	O-DEB-DEBI-060919/496
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://lists.xymon.com/archive/2019-July/046570.html	O-DEB-DEBI-060919/497
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 reportlog.c. **CVE ID : CVE-2019-13452**	https://lists.xymon.com/archive/2019-July/046570.html	O-DEB-DEBI-060919/498
Improper Restriction of Operations within the Bounds of a Memory	27-08-2019	7.5	In Xymon through 4.3.28, a stack-based buffer overflow vulnerability exists in the alert acknowledgment CGI tool because of &nbsp; expansion in acknowledge.c. **CVE ID : CVE-2019-13455**	https://lists.xymon.com/archive/2019-July/046570.html	O-DEB-DEBI-060919/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer					
N/A	21-08-2019	4	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.8, and Community Edition 5.0.x through 5.0.36 and 6.0.x through 6.0.19. An attacker who is logged into OTRS as an agent user with appropriate permissions can leverage OTRS notification tags in templates in order to disclose hashed user passwords. **CVE ID : CVE-2019-13458**	N/A	O-DEB-DEBI-060919/500
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 re-connection, 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. **CVE ID : CVE-2019-15239**	N/A	O-DEB-DEBI-060919/501
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	N/A	O-DEB-DEBI-060919/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC 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_firmware					
Improper Neutralization 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	O-DLI-DIR--060919/503
Improper Neutralization 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	O-DLI-DIR--060919/504
Improper Neutralization of Special Elements used in a Command ('Command	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 Interface field to	N/A	O-DLI-DIR--060919/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			SetStaticRouteSettings. **CVE ID : CVE-2019-15528**		
Improper Neutralization 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 Username field to Login. **CVE ID : CVE-2019-15529**	N/A	O-DLI-DIR--060919/506
Improper Neutralization 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 LoginPassword field to Login. **CVE ID : CVE-2019-15530**	N/A	O-DLI-DIR--060919/507
galliumos					
galliumos					
N/A	22-08-2019	5	In GalliumOS 3.0, CONFIG_SECURITY_YAMA is disabled but /etc/sysctl.d/10-ptrace.conf tries to set /proc/sys/kernel/yama/ptrace_scope to 1, which might increase risk because of the appearance that a protection mechanism is present when actually it is not. **CVE ID : CVE-2019-15325**	N/A	O-GAL-GALL-060919/508
getvera					
vera_edge_firmware					
Improper Neutralization of Special	23-08-2019	9.3	cgi-bin/cmh/webcam.sh in Vera Edge Home Controller 1.7.4452 allows remote unauthenticated users to execute arbitrary OS	N/A	O-GET-VERA-060919/509

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
Elements used in an OS Command ('OS Command Injection')			commands via --output argument injection in the username parameter to /cgi-bin/cmh/webcam.sh. **CVE ID : CVE-2019-15498**		
Google					
nest_cam_iq_indoor_firmware					
Out-of-bounds Read	20-08-2019	5	An exploitable information disclosure vulnerability exists in the Weave Legacy Pairing functionality of Nest Cam IQ Indoor version 4620002. A set of specially crafted weave packets can cause an out of bounds read, resulting in information disclosure. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2019-5034**	N/A	O-GOO-NEST-060919/510
Improper Authentication	20-08-2019	6.8	An exploitable information disclosure vulnerability exists in the Weave PASE pairing functionality of the Nest Cam IQ Indoor, version 4620002. A set of specially crafted weave packets can brute force a pairing code, resulting in greater Weave access and potentially full device control. An attacker can send specially crafted packets to trigger this vulnerability. **CVE ID : CVE-2019-5035**	N/A	O-GOO-NEST-060919/511
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	N/A	O-GOO-NEST-060919/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			weave packets can cause an arbitrary Weave Exchange Session to close, resulting in a denial of service. An attacker can send a specially crafted packet to trigger this vulnerability. **CVE ID : CVE-2019-5036**		
Integer Overflow or Wraparound	20-08-2019	7.8	An exploitable denial-of-service vulnerability exists in the Weave certificate loading functionality of Nest Cam IQ Indoor camera, version 4620002. A specially crafted weave packet can cause an integer overflow and an out-of-bounds read on unmapped memory to occur, resulting in a denial of service. An attacker can send a specially crafted packet to trigger. **CVE ID : CVE-2019-5037**	N/A	O-GOO-NEST-060919/513
Integer Overflow or Wraparound	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-GOO-NEST-060919/514
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://source.android.com/security/bulletin/20	O-GOO-ANDR-060919/515

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. **CVE ID : CVE-2019-2129**	https://source.android.com/security/bulletin/2019-08-01	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://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/517

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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. **CVE ID : CVE-2019-2131**	https://source.android.com/security/bulletin/2019-08-01	O-GOO-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. **CVE ID : CVE-2019-2132**	https://source.android.com/security/bulletin/2019-08-01	O-GOO-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://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/520

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
Integer Overflow or Wraparound	20-08-2019	9.3	In phFriNfc_ExtnsTransceive of phNxpExtns_MifareStd.cpp, there is a possible out of bounds write due to an integer 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-132083376. **CVE ID : CVE-2019-2134**	https://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/521
Out-of-bounds Read	20-08-2019	7.1	In Mfc_Transceive of phNxpExtns_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-125900276. **CVE ID : CVE-2019-2135**	https://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/522
Out-of-bounds Read	20-08-2019	4.9	In Status::readFromParcel of Status.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure 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	https://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/523

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
			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://source.android.com/security/bulletin/2019-08-01	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://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/525
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	20-08-2019	6.9	In ActivityManagerService.attachApplication 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://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			exploitation. Product: Android. Versions: Android-9. Android ID: A-131105245. **CVE ID : CVE-2019-2121**		
N/A	20-08-2019	6.9	In LockTaskController.lockKeyguardIfNeeded 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. **CVE ID : CVE-2019-2122**	https://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/527
N/A	20-08-2019	4.4	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. 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. **CVE ID : CVE-2019-2125**	https://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/528
Double	20-08-2019	9.3	In ParseContentEncodingEntry of	https://so	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			mkvparser.cc, there is a possible double free due to a missing reset of a freed pointer. This could lead to remote code execution 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-127702368. **CVE ID : CVE-2019-2126**	urce.android.com/security/bulletin/2019-08-01	ANDR-060919/529
Use After Free	20-08-2019	7.2	In AudioInputDescriptor::setClientActive of AudioInputDescriptor.cpp, there is possible memory corruption due to a use after free. 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-124899895. **CVE ID : CVE-2019-2127**	https://source.android.com/security/bulletin/2019-08-01	O-GOO-ANDR-060919/530
Intel					
compute_card_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://www.intel.com/content/www/us/en/security-center/advisory/int	O-INT-COMP-060919/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				el-sa-00272.html	
compute_stick_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://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00272.html	O-INT-COMP-060919/532
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://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00272.html	O-INT-NUC_-060919/533
Lenovo					
20ng_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-20NG-060919/534

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
20nn_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-20NN-060919/535
20nq_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-20NQ-060919/536
20nr_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-20NR-060919/537
20ns_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	N/A	O-LEN-20NS-060919/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware. **CVE ID : CVE-2019-6171**		
20nt_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-20NT-060919/539
20nu_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-20NU-060919/540
230x_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-230X-060919/541
232x_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	N/A	O-LEN-232X-060919/542

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_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-233X-060919/543
234x_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-234X-060919/544
235x_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-235X-060919/545
239x_firmware					
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	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		060919/546
242x_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-242X-060919/547
243x_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-243X-060919/548
244x_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-244X-060919/549

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
246x_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-246X-060919/550
247x_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-247X-060919/551
248x_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-248X-060919/552
30eh_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	N/A	O-LEN-30EH-060919/553

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
			firmware. **CVE ID : CVE-2019-6171**		
336x_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-336X-060919/554
337x_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-337X-060919/555
343x_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-343X-060919/556
344x_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	N/A	O-LEN-344X-060919/557

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
			privileges or physical access the ability to update the Embedded Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
34xx_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-34XX-060919/558
3xxx_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-3XXX-060919/559
home_media_network_hard_drive_firmware					
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-HOME-060919/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ix12-300r_firmware					
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_firmware					
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_firmware					
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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6178		
storecenter_ix4-200d_firmware					
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-STOR-060919/564
storecenter_ix4-200rl_firmware					
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-STOR-060919/565
bladecenter_hs22_firmware					
Improper Neutralization 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	O-LEN-BLAD-060919/566

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_firmware					
Improper Neutralization 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_firmware					
Improper Neutralization 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

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. **CVE ID : CVE-2019-6159**		
system_x3400_m3_firmware					
Improper Neutralization 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-060919/569
system_x3500_m2_firmware					
Improper Neutralization 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

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_x3500_m3_firmware					
Improper Neutralization 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-060919/571
system_x3550_m3_firmware					
Improper Neutralization 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	N/A	O-LEN-SYST-060919/572

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
			not executed on IMM itself. The later IMM2 (IMM v2) is not affected. **CVE ID : CVE-2019-6159**		
system_x3560_m2_firmware					
Improper Neutralization 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-060919/573
system_x3630_m3_firmware					
Improper Neutralization 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	N/A	O-LEN-SYST-060919/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			later IMM2 (IMM v2) is not affected. **CVE ID : CVE-2019-6159**		
system_x3650_m3_firmware					
Improper Neutralization 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-060919/575
system_x3690_x5_firmware					
Improper Neutralization 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	O-LEN-SYST-060919/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected. **CVE ID : CVE-2019-6159**		
system_x3850_x5_firmware					
Improper Neutralization 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-060919/577
system_x3950_x5_firmware					
Improper Neutralization 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	O-LEN-SYST-060919/578

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6159		
system_x_idataplex_dx360_m2_firmware					
Improper Neutralization 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_idataplex_dx360_m3_firmware					
Improper Neutralization 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	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
yoga_700-11isk_firmware					
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_700-14isk_firmware					
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_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-20A7-060919/583
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	1-2	2-3	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_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-20A9-060919/585
20aa_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-20AA-060919/586
20ab_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-20AB-060919/587
20ac_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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-20AC-060919/588
20aj_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-20AJ-060919/589
20ak_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-20AK-060919/590
20al_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.	N/A	O-LEN-20AL-060919/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20am_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-20AM-060919/592
20an_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-20AN-060919/593
20aq_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-20AQ-060919/594
20ar_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	N/A	O-LEN-20AR-060919/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20aw_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-20AW-060919/596
20b0_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-20B0-060919/597
20b3_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-20B3-060919/598
20b6_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-20B6-060919/599

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_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-20B7-060919/600
20be_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-20BE-060919/601
20bf_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-20BF-060919/602
20bg_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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-20BG-060919/603
20bl_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-20BL-060919/604
20bm_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-20BM-060919/605
20bu_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.	N/A	O-LEN-20BU-060919/606

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20bv_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-20BV-060919/607
20bw_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-20BW-060919/608
20bx_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-20BX-060919/609
20d9_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	N/A	O-LEN-20D9-060919/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20da_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-20DA-060919/611
20dc_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-20DC-060919/612
20dd_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-20DD-060919/613
20de_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-20DE-060919/614

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**		
20df_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-20DF-060919/615
20dg_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-20DG-060919/616
20dh_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-20DH-060919/617
20dj_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-20DJ-060919/618
20dq_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-20DQ-060919/619
20dr_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-20DR-060919/620
20ds_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.	N/A	O-LEN-20DS-060919/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20dt_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-20DT-060919/622
20e0_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-20E0-060919/623
20ef_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-20EF-060919/624
20eg_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	N/A	O-LEN-20EG-060919/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20et_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-20ET-060919/626
20eu_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-20EU-060919/627
20ev_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-20EV-060919/628
20ew_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-20EW-060919/629

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_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-20EX-060919/630
20ey_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-20EY-060919/631
20f1_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-20F1-060919/632
20f2_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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-20F2-060919/633
20f5_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-20F5-060919/634
20f6_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-20F6-060919/635
20fm_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.	N/A	O-LEN-20FM-060919/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20fn_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-20FN-060919/637
20fu_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-20FU-060919/638
20fv_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-20FV-060919/639
20fw_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	N/A	O-LEN-20FW-060919/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20fx_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-20FX-060919/641
20g4_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-20G4-060919/642
20g5_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-20G5-060919/643
20g8_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-20G8-060919/644

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**		
20g9_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-20G9-060919/645
20ga_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-20GA-060919/646
20gb_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-20GB-060919/647
20h1_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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-20H1-060919/648
20h2_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-20H2-060919/649
20h4_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-20H4-060919/650
20h5_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.	N/A	O-LEN-20H5-060919/651

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20h6_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-20H6-060919/652
20h8_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-20H8-060919/653
20hm_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-20HM-060919/654
20hn_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	N/A	O-LEN-20HN-060919/655

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
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20hs_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-20HS-060919/656
20ht_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-20HT-060919/657
20hu_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-20HU-060919/658
20hv_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-20HV-060919/659

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_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-20J1-060919/660
20j2_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-20J2-060919/661
20j4_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-20J4-060919/662
20j5_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-20J5-060919/663
20j6_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-20J6-060919/664
20j7_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-20J7-060919/665
20ja_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.	N/A	O-LEN-20JA-060919/666

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20jh_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-20JH-060919/667
20jj_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-20JJ-060919/668
20jq_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-20JQ-060919/669
20jr_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	N/A	O-LEN-20JR-060919/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20ju_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-20JU-060919/671
20jv_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-20JV-060919/672
20k5_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-20K5-060919/673
20k6_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-20K6-060919/674

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_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-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_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-20KL-060919/677
20km_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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-20KM-060919/678
20kn_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-20KN-060919/679
20kq_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-20KQ-060919/680
20ks_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.	N/A	O-LEN-20KS-060919/681

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20kt_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-20KT-060919/682
20ku_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-20KU-060919/683
20kv_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-20KV-060919/684
20l2_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	N/A	O-LEN-20L2-060919/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20lh_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-20LH-060919/686
20lj_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-20LJ-060919/687
20lm_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-20LM-060919/688
20ln_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-20LN-060919/689

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_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-20LQ-060919/690
20lr_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-20LR-060919/691
20ls_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-20LS-060919/692
20lt_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-20LT-060919/693
20lx_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-20LX-060919/694
20m5_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-20M5-060919/695
20m6_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.	N/A	O-LEN-20M6-060919/696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6171		
20m7_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-20M7-060919/697
20m8_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-20M8-060919/698
20mu_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-20MU-060919/699
20mv_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	N/A	O-LEN-20MV-060919/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller with unsigned firmware. **CVE ID : CVE-2019-6171**		
20mw_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-20MW-060919/701
20mx_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-20MX-060919/702
20n8_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-20N8-060919/703
20n9_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-20N9-060919/704

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**		
Lexmark					
c925_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-C925-060919/705
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-C925-060919/706
c950_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-C950-060919/707

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
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-C950-060919/708
cs51x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-CS51-060919/709
cs748_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-CS74-060919/710
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&user	O-LEX-CS74-060919/711

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
				locale=EN_US	
cs796_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-CS79-060919/712
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-CS79-060919/713
e46x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-E46X-060919/714
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=conten	O-LEX-E46X-060919/715

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
				t&id=TE920&locale=EN&userlocale=EN_US	
m3150_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-M315-060919/716
m5155_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-M515-060919/717
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-M515-060919/718
m5163_firmware					
Improper	28-08-2019	6.4	Various Lexmark products have	http://su	O-LEX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			Incorrect Access Control. **CVE ID : CVE-2019-10058**	pport.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	M516-060919/719
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-M516-060919/720
m5170_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-M517-060919/721
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ms610de_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS61-060919/723
ms810de_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/724
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/725
ms812de_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE9	O-LEX-MS81-060919/726

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
				22&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/727
ms91x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS91-060919/728
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS91-060919/729
t65x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com	O-LEX-T65X-060919/730

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?page=content&id=TE922&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-T65X-060919/731
w850_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-W850-060919/732
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-W850-060919/733
xm51xx_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-XM51-060919/734
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-XM51-060919/735
xm71xx_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-XM71-060919/736
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN	O-LEX-XM71-060919/737

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
		🟥		_US	
cs31x_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-CS31-060919/739
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-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://support.lexmark.com/index?page=content&id=TE924&locale=en&userl	O-LEX-CS31-060919/741

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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-CS31-060919/742
cs41x_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-CS41-060919/744
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&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	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				=EN&userlocale=EN_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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-CS41-060919/746
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-CS41-060919/747
m1140_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-M114-060919/748
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE9	O-LEX-M114-060919/749

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
				22&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-M114-060919/750
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-M114-060919/751
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-M114-060919/752
m1145_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=conten	O-LEX-M114-060919/753

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
				t&id=TE921&locale=EN&userlocale=EN_US	
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-M114-060919/754
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-M114-060919/755
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-M114-060919/756
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=conten	O-LEX-M114-060919/757

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
				t&id=TE924&locale=EN&userlocale=EN_US	
m3150dn_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-M315-060919/759
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?pa	O-LEX-M315-060919/761

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9934	ge=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-M315-060919/762
m5163dn_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-M516-060919/763
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-M516-060919/764
Integer Overflow or Wraparoun	28-08-2019	10	Various Lexmark products have an Integer Overflow.	http://support.lexmark.com	O-LEX-M516-

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
d			**CVE ID : CVE-2019-9930**	/index?page=content&id=TE920&locale=EN&userlocale=EN_US	060919/765
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-M516-060919/766
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-M516-060919/767
ms310_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/768
Improper Access	28-08-2019	6.4	Various Lexmark products have	http://support.lex	O-LEX-MS31-

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
Control			Incorrect Access Control. **CVE ID : CVE-2019-10058**	mark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	060919/769
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/772
ms312_firmware					

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
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/773
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/774
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/775
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS31-060919/776

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/777
ms315_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/778
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/779
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN	O-LEX-MS31-060919/780

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				_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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/782
ms317_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&user	O-LEX-MS31-060919/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				locale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS31-060919/787
ms410_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&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	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				=EN&userlocale=EN_US	
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS41-060919/789
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS41-060919/790
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS41-060919/791
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale	O-LEX-MS41-060919/792

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
				=EN&userlocale=EN_US	
ms415_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS41-060919/794
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?page=content&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	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				24&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS41-060919/797
ms417_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MS41-060919/798
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS41-060919/799
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=conten	O-LEX-MS41-060919/800

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
				t&id=TE920&locale=EN&userlocale=EN_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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS41-060919/801
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS41-060919/802
ms51x_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MS51-060919/803
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?pa	O-LEX-MS51-060919/804

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
				ge=content&id=TE922&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS51-060919/805
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS51-060919/806
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS51-060919/807
ms610dn_firmware					
Cross-Site Request Forgery	28-08-2019	4.3	Various Lexmark products have CSRF.	http://support.lexmark.com	O-LEX-MS61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			**CVE ID : CVE-2019-10057**	/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS61-060919/809
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=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://support.lexmark.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	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9935	/index?page=content&id=TE924&locale=EN&userlocale=EN_US	
ms617_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS61-060919/814
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS61-060919/815
Improper Access	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1	http://support.lex	O-LEX-MS61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			of 2). **CVE ID : CVE-2019-9934**	mark.com/index?page=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS61-060919/817
ms71x_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS71-060919/819

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
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS71-060919/822
ms810_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN	O-LEX-MS81-060919/823

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
				_US	
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/824
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/825
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS81-060919/826
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN	O-LEX-MS81-060919/827

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
				_US	
ms811_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/829
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=en&userl	O-LEX-MS81-060919/831

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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/832
ms812_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/833
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/834
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale	O-LEX-MS81-060919/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				=EN&userlocale=EN_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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS81-060919/836
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/837
ms817_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/838
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE9	O-LEX-MS81-060919/839

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
				22&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/840
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS81-060919/841
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/842
ms818_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=conten	O-LEX-MS81-060919/843

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
				t&id=TE921&locale=EN&userlocale=EN_US	
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/844
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MS81-060919/845
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-MS81-060919/846
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=conten	O-LEX-MS81-060919/847

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
				t&id=TE924&locale=EN&userlocale=EN_US	
xm1135_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=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://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-XM11-060919/849
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=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://support.lexmark.com/index?pa	O-LEX-XM11-060919/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9934	ge=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-XM11-060919/852
c734_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-C734-060919/853
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-C734-060919/854
c736_firmware					
Improper	28-08-2019	6.4	Various Lexmark products have	http://su	O-LEX-C736-

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.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	060919/855
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-C736-060919/856
c746_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-C746-060919/857
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-C746-060919/858

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
c748_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-C748-060919/859
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-C748-060919/860
c792_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-C792-060919/861
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&user	O-LEX-C792-060919/862

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
				locale=EN_US	
x86x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X86X-060919/863
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-X86X-060919/864
x925_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X925-060919/865
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=conten	O-LEX-X925-060919/866

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
				t&id=TE920&locale=EN&userlocale=EN_US	
x95x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X95X-060919/867
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-X95X-060919/868
xm3150_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-XM31-060919/869
Integer Overflow or	28-08-2019	10	Various Lexmark products have an Integer Overflow.	http://support.lex	O-LEX-XM31-

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
Wraparound			**CVE ID : CVE-2019-9930**	mark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	060919/870
xm91x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-XM91-060919/871
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-XM91-060919/872
xs548_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN	O-LEX-XS54-060919/873

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
				_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-XS54-060919/874
xs748_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-XS74-060919/875
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-XS74-060919/876
xs79x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE9	O-LEX-XS79-060919/877

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
				22&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-XS79-060919/878
xs925_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-XS92-060919/879
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-XS92-060919/880
xs95x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com	O-LEX-XS95-060919/881

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?page=content&id=TE922&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-XS95-060919/882
6500e_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-6500-060919/883
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-6500-060919/884
cx310_firmware					

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
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-CX31-060919/885
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-CX31-060919/886
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-CX31-060919/887
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 1 of 2). **CVE ID : CVE-2019-9934**	http://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=EN_US	O-LEX-CX31-060919/888

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	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	28-08-2019	5	Various Lexmark products have Incorrect Access Control (issue 2 of 2). **CVE ID : CVE-2019-9935**	http://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-CX31-060919/889
mx31x_firmware					
Cross-Site Request Forgery (CSRF)	28-08-2019	4.3	Various Lexmark products have CSRF. **CVE ID : CVE-2019-10057**	http://support.lexmark.com/index?page=content&id=TE921&locale=EN&userlocale=EN_US	O-LEX-MX31-060919/890
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX31-060919/891
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN	O-LEX-MX31-060919/892

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
				_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://support.lexmark.com/index?page=content&id=TE924&locale=en&userlocale=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://support.lexmark.com/index?page=content&id=TE924&locale=EN&userlocale=EN_US	O-LEX-MX31-060919/894
mx410_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX41-060919/895
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&user	O-LEX-MX41-060919/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟥		locale=EN_US	
mx510_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX51-060919/897
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MX51-060919/898
mx511_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX51-060919/899
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=conten	O-LEX-MX51-060919/900

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
				t&id=TE920&locale=EN&userlocale=EN_US	
mx610_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX61-060919/901
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MX61-060919/902
mx611_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX61-060919/903
Integer Overflow or	28-08-2019	10	Various Lexmark products have an Integer Overflow.	http://support.lex	O-LEX-MX61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			**CVE ID : CVE-2019-9930**	mark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	060919/904
mx6500e_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX65-060919/905
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MX65-060919/906
mx71x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN	O-LEX-MX71-060919/907

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
				_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MX71-060919/908
mx81x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-MX81-060919/909
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MX81-060919/910
mx91x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE9	O-LEX-MX91-060919/911

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
				22&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-MX91-060919/912
x46x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X46X-060919/913
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-X46X-060919/914
x548_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com	O-LEX-X548-060919/915

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?page=content&id=TE922&locale=EN&userlocale=EN_US	
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-X548-060919/916
x65x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X65X-060919/917
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-X65X-060919/918
x73x_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X73X-060919/919
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-X73X-060919/920
x74x_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X74X-060919/921
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN	O-LEX-X74X-060919/922

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
				_US	
x792_firmware					
Improper Access Control	28-08-2019	6.4	Various Lexmark products have Incorrect Access Control. **CVE ID : CVE-2019-10058**	http://support.lexmark.com/index?page=content&id=TE922&locale=EN&userlocale=EN_US	O-LEX-X792-060919/923
Integer Overflow or Wraparound	28-08-2019	10	Various Lexmark products have an Integer Overflow. **CVE ID : CVE-2019-9930**	http://support.lexmark.com/index?page=content&id=TE920&locale=EN&userlocale=EN_US	O-LEX-X792-060919/924
Linux					
linux_kernel					
Double Free	23-08-2019	10	drivers/net/wireless/rsi/rsi_91x_usb.c in the Linux kernel through 5.2.9 has a Double Free via crafted USB device traffic (which may be remote via usbip or usbredir). **CVE ID : CVE-2019-15504**	N/A	O-LIN-LINU-060919/925
Out-of-bounds Read	23-08-2019	10	drivers/media/usb/dvb-usb/technisat-usb2.c in the Linux kernel through 5.2.9 has an out-of-bounds read via crafted USB device traffic (which may be remote via usbip or usbredir). **CVE ID : CVE-2019-15505**	N/A	O-LIN-LINU-060919/926

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper 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
Uncontrolled Resource Consumption	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	O-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 Dereference	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 Dereference	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 Dereference	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

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
			b.c driver. **CVE ID : CVE-2019-15218**		
NULL Pointer Dereference	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/sisusb.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/p54/p54usb.c driver. **CVE ID : CVE-2019-15220**	N/A	O-LIN-LINU-060919/938
NULL Pointer Dereference	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 Dereference	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 Dereference	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 re-connection, 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. **CVE ID : CVE-2019-15239**	N/A	O-LIN-LINU-060919/942
NULL Pointer Dereference	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	O-LIN-LINU-060919/943
NULL Pointer Dereference	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	Description & CVE ID	Patch	NCIIPC ID
			drivers/media/usb/b2c2/flexcop-usb.c driver. **CVE ID : CVE-2019-15291**		
Use After Free	21-08-2019	10	An issue was discovered in the Linux kernel before 5.0.9. There is a use-after-free in atalk_proc_exit, related to net/appletalk/atalk_proc.c, net/appletalk/ddp.c, and net/appletalk/sysctl_net_atalk.c. **CVE ID : CVE-2019-15292**	N/A	O-LIN-LINU-060919/945
Out-of-bounds Read	27-08-2019	7.8	An issue was discovered in the Linux kernel before 5.0.19. There is an out-of-bounds array access in __xfrm_policy_unlink, which will cause denial of service, because verify_newpolicy_info in net/xfrm/xfrm_user.c mishandles directory validation. **CVE ID : CVE-2019-15666**	N/A	O-LIN-LINU-060919/946
Motorola					
cx2l_mwr04l_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. **CVE ID : CVE-2019-15513**	N/A	O-MOT-CX2L-060919/947
c1_mwr03_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	N/A	O-MOT-C1_M-060919/948

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
			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**		
Paloaltonetworks					
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://securityadvisories.paloaltonetworks.com/home/detail/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://securityadvisories.paloaltonetworks.com/home/detail/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://securityadvisories.paloaltonetworks.com/home/detail/161	O-PAL-PAN--060919/951
Tp-link					

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
tl-wr840n_firmware					
Improper Input Validation	22-08-2019	6.5	The traceroute function on the TP-Link TL-WR840N v4 router with firmware through 0.9.1 3.16 is vulnerable to remote code execution via a crafted payload in an IP address input field. **CVE ID : CVE-2019-15060**	N/A	O-TP--TL-W-060919/952
zebra					
220xi4_firmware					
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-220X-060919/953
zt220_firmware					
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	N/A	O-ZEB-ZT22-060919/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
zt230_firmware					
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-ZT23-060919/955
zt410_firmware					
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	N/A	O-ZEB-ZT41-060919/956

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
			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**		
zt420_firmware					
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-ZT42-060919/957
zt510_firmware					
N/A	20-08-2019	5	Zebra Industrial Printers All Versions, Zebra printers are	N/A	O-ZEB-ZT51-060919/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
zt610_firmware					
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 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-ZT62-060919/960