National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 31 May 2019 Vol. 06 No. 10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Adobe					
acrobat					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7085**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/1
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7086**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/2
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/3

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
			arbitrary code execution . **CVE ID : CVE-2019-7087**		
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7088**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/4
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7089**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/5
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7018**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/6
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/7

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7019**	acrobat/apsb19-07.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7020**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/8
Use After Free	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7021**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/9
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-7022		
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7023**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/11
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7024**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/12
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7025**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/13
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/14

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7026**	b19-07.html	
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7027**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/15
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7028**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/16
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7029**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/17

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7030**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/18
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7031**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/19
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7032**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/20
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7033**	07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7034**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/22
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7035**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/23
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7036**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7037**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/25
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7038**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/26
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7039**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/27
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7040**	07.html	
N/A	24-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-7041**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/29
NULL Pointer Dereference	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7042**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/30
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7043**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/31

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7044**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/32
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7045**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/33
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7046**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/34
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/35

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7047**	b19-07.html	
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7048**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/36
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7049**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/37
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7050**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/38

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7051**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/39
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7052**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/40
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7053**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/41
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7054**	b19-07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7055**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/43
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7056**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/44
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7057		
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7058**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/46
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7059**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/47
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7060**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/48
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7061**	b19-17.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7062**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/50
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7063**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/51
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7064**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/52

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7065**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/53
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7066**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/54
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7067**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/55
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7068**	b19-07.html	
Incorrect Type Conversion or Cast	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7069**	N/A	A-ADO-ACRO-060619/57
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7070**	N/A	A-ADO-ACRO-060619/58
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7071**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/59

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7072**	N/A	A-ADO-ACRO-060619/60
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7073**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/61
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7074**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/62
Use After Free	24-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7075**	07.html	
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7076**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/64
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7077**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/65
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7078**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/66

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Write	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7079**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/67
Double Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7080**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/68
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7081**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/69
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7082**	07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7083**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/71
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7084**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/72
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7109**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7110**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/74
Out-of-bounds Write	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7111**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/75
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7112**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/76
Improper Restriction of Operations within the	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7113**	17.html	
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7114**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/78
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7115**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/79
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7116**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7117**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/81
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7118**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/82
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7119**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/83
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/84

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7120**	17.html	
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7121**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/85
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7122**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/86
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7123**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7124**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/88
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7125**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/89
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7127**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/90
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7128**	17.html	
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7140**	N/A	A-ADO-ACRO-060619/92
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7141**	N/A	A-ADO-ACRO-060619/93
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure . **CVE ID : CVE-2019-7142**		
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7143**	N/A	A-ADO-ACRO-060619/95
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7144**	N/A	A-ADO-ACRO-060619/96
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7145**	N/A	A-ADO-ACRO-060619/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7758**	N/A	A-ADO-ACRO-060619/98
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7759**	N/A	A-ADO-ACRO-060619/99
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7760**	N/A	A-ADO-ACRO-060619/100
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-060619/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7761**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7762**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/102
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7763**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/103
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version,	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7764**	b19-18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7765**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/105
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7766**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/106
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7767**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7768**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/108
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7769**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/109
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2019-7770**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7771**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/111
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7772**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/112
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7773**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7774**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/114
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7775**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/115
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7776**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/116
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	https://helpx.adobe.com/security	A-ADO-ACRO-060619/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7777**	/products/acrobat/apsb19-18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7778**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/118
N/A	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7779**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/119
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7780**	18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7781**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/121
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7782**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/122
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7783**		
Double Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7784**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/124
Use After Free	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7785**	N/A	A-ADO-ACRO-060619/125
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	N/A	A-ADO-ACRO-060619/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7786		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7787**	N/A	A-ADO-ACRO-060619/127
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7788**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/128
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7789**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/129
Out-of-	22-05-2019	5	Adobe Acrobat and Reader	https://hel	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7790**	px.adobe.com/security/products/acrobat/apsb19-18.html	060619/130
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7791**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/131
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7792**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/132
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7793**	acrobat/apsb19-18.html	
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7794**	N/A	A-ADO-ACRO-060619/134
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7795**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/135
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	N/A	A-ADO-ACRO-060619/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7796**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7797**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/137
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7798**	N/A	A-ADO-ACRO-060619/138
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-	N/A	A-ADO-ACRO-060619/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7799**		
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7800**	N/A	A-ADO-ACRO-060619/140
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7801**	N/A	A-ADO-ACRO-060619/141
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	N/A	A-ADO-ACRO-060619/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2019-7802**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7803**	N/A	A-ADO-ACRO-060619/143
Out-of-bounds Write	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7804**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/144
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7805		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7806**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/146
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7807**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/147
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7808**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/148
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-060619/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7809**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7810**	N/A	A-ADO-ACRO-060619/150
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7811**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/151
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7812**	b19-18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7813**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/153
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7814**	N/A	A-ADO-ACRO-060619/154
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20091 and earlier, 2019.010.20091 and earlier, 2017.011.30120 and earlier version, and 2015.006.30475 and earlier have a data leakage (sensitive) vulnerability. Successful	https://helpx.adobe.com/security/products/acrobat/apsb19-13.html	A-ADO-ACRO-060619/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to information disclosure. **CVE ID : CVE-2019-7815**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7817**	N/A	A-ADO-ACRO-060619/156
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7818**	N/A	A-ADO-ACRO-060619/157
Incorrect Type Conversion or Cast	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code	N/A	A-ADO-ACRO-060619/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-7820**		
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7821**	N/A	A-ADO-ACRO-060619/159
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7822**	N/A	A-ADO-ACRO-060619/160
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	N/A	A-ADO-ACRO-060619/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7823		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7824**	N/A	A-ADO-ACRO-060619/162
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7825**	N/A	A-ADO-ACRO-060619/163
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7826**	N/A	A-ADO-ACRO-060619/164
Improper	22-05-2019	9.3	Adobe Acrobat and Reader	N/A	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7827**		060619/165
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7828**	N/A	A-ADO-ACRO-060619/166
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7829**	N/A	A-ADO-ACRO-060619/167
Use After	22-05-2019	9.3	Adobe Acrobat and Reader	N/A	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7830**		060619/168
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7831**	N/A	A-ADO-ACRO-060619/169
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7832**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/170
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7833**	acrobat/apsb19-18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7834**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/172
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7835**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/173
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7836**	18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7841**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/175
acrobat_dc					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7085**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/176
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2019-7086**		
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7087**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/178
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7088**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/179
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7089**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/180
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7018**	acrobat/apsb19-07.html	
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7019**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/182
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7020**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/183
Use After Free	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7021		
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7022**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/185
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7023**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/186
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7024**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/187
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7025**	b19-07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7026**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/189
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7027**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/190
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7028**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/191

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7029**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/192
Integer Overflow or Wraparound	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7030**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/193
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7031**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/194
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7032**	07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7033**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/196
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7034**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/197
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7035**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7036**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/199
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7037**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/200
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7038**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/201
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7039**	07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7040**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/203
N/A	24-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-7041**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/204
NULL Pointer Dereference	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7042**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/205

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7043**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/206
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7044**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/207
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7045**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/208
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7046**	07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7047**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/210
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7048**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/211
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7049**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/212

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7050**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/213
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7051**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/214
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7052**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/215
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/216

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7053**	b19-07.html	
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7054**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/217
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7055**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/218
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7056		
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7057**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/220
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7058**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/221
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7059**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/222
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7060**	b19-07.html	
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7061**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/224
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7062**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/225
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7063**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/226

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
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7064**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/227
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7065**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/228
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7066**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/229
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7067**	b19-07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7068**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/231
Incorrect Type Conversion or Cast	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7069**	N/A	A-ADO-ACRO-060619/232
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7070**	N/A	A-ADO-ACRO-060619/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7071**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/234
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7072**	N/A	A-ADO-ACRO-060619/235
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7073**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/236
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7074**	07.html	
Use After Free	24-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7075**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/238
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7076**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/239
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7077**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7078**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/241
Out-of-bounds Write	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7079**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/242
Double Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7080**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/243
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7081**	07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7082**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/245
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7083**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/246
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7084**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7109**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/248
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7110**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/249
Out-of-bounds Write	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7111**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/250
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7112**	17.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7113**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/252
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7114**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/253
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7115**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7116**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/255
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7117**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/256
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7118**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/257
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7119**	17.html	
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7120**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/259
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7121**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/260
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7122**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7123**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/262
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7124**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/263
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7125**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/264
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7127**	17.html	
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7128**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/266
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7140**	N/A	A-ADO-ACRO-060619/267
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	N/A	A-ADO-ACRO-060619/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7141		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7142**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/269
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7143**	N/A	A-ADO-ACRO-060619/270
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7144**	N/A	A-ADO-ACRO-060619/271
Out-of-bounds	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-060619/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7145**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7758**	N/A	A-ADO-ACRO-060619/273
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7759**	N/A	A-ADO-ACRO-060619/274
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	N/A	A-ADO-ACRO-060619/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7760**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7761**	N/A	A-ADO-ACRO-060619/276
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7762**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/277
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7763**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7764**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/279
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7765**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/280
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7766**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7767**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/282
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7768**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/283
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7769**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/284

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7770**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/285
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7771**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/286
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7772**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/287
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	https://helpx.adobe.com/security	A-ADO-ACRO-060619/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7773**	/products/acrobat/apsb19-18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7774**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/289
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7775**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/290
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7776**	18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7777**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/292
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7778**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/293
N/A	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a security bypass vulnerability. Successful	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7779**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7780**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/295
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7781**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/296
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7782		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7783**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/298
Double Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7784**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/299
Use After Free	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7785**	N/A	A-ADO-ACRO-060619/300
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-060619/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7786**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7787**	N/A	A-ADO-ACRO-060619/302
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7788**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/303
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7789**	acrobat/apsb19-18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7790**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/305
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7791**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/306
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7792**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7793**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/308
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7794**	N/A	A-ADO-ACRO-060619/309
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2019-7795**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7796**	N/A	A-ADO-ACRO-060619/311
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7797**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/312
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7798**	N/A	A-ADO-ACRO-060619/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7799**	N/A	A-ADO-ACRO-060619/314
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7800**	N/A	A-ADO-ACRO-060619/315
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7801**	N/A	A-ADO-ACRO-060619/316
Out-of-	22-05-2019	4.3	Adobe Acrobat and Reader	N/A	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7802**		060619/317
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7803**	N/A	A-ADO-ACRO-060619/318
Out-of-bounds Write	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7804**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/319
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and	https://helpx.adobe.co	A-ADO-ACRO-060619/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7805**	m/security/products/acrobat/apsb19-18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7806**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/321
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7807**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/322
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7808**	b19-18.html	
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7809**	N/A	A-ADO-ACRO-060619/324
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7810**	N/A	A-ADO-ACRO-060619/325
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7811**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7812**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/327
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7813**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/328
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	N/A	A-ADO-ACRO-060619/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7814		
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20091 and earlier, 2019.010.20091 and earlier, 2017.011.30120 and earlier version, and 2015.006.30475 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7815**	https://helpx.adobe.com/security/products/acrobat/apsb19-13.html	A-ADO-ACRO-060619/330
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7817**	N/A	A-ADO-ACRO-060619/331
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7818**	N/A	A-ADO-ACRO-060619/332
Incorrect Type	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-060619/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7820**		
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7821**	N/A	A-ADO-ACRO-060619/334
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7822**	N/A	A-ADO-ACRO-060619/335
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	N/A	A-ADO-ACRO-060619/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7823**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7824**	N/A	A-ADO-ACRO-060619/337
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7825**	N/A	A-ADO-ACRO-060619/338
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	N/A	A-ADO-ACRO-060619/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7826**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7827**	N/A	A-ADO-ACRO-060619/340
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7828**	N/A	A-ADO-ACRO-060619/341
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and	N/A	A-ADO-ACRO-060619/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7829**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7830**	N/A	A-ADO-ACRO-060619/343
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7831**	N/A	A-ADO-ACRO-060619/344
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7832**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7833**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/346
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7834**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/347
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7835**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7836**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/349
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7841**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/350
acrobat_reader					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7085		
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7086**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/352
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7087**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/353
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7088**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/354
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7089**	b19-07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7018**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/356
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7019**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/357
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7020**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/358

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7021**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/359
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7022**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/360
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7023**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/361
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7024**	07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7025**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/363
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7026**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/364
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7027**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7028**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/366
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7029**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/367
Integer Overflow or Wraparound	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7030**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/368
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7031**	07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7032**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/370
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7033**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/371
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7034**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7035**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/373
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7036**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/374
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7037**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/375
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7038**	07.html	
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7039**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/377
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7040**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/378
N/A	24-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-7041**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7042**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/380
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7043**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/381
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7044**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/382
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7045**	b19-07.html	
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7046**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/384
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7047**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/385
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7048		
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7049**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/387
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7050**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/388
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7051**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/389
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7052**	acrobat/apsb19-07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7053**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/391
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7054**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/392
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2019-7055**		
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7056**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/394
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7057**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/395
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7058**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/396
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7059**	acrobat/apsb19-07.html	
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7060**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/398
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7061**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/399
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7062		
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7063**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/401
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7064**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/402
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7065**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/403
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7066**	b19-07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7067**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/405
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7068**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/406
Incorrect Type Conversion or Cast	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution .	N/A	A-ADO-ACRO-060619/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7069		
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7070**	N/A	A-ADO-ACRO-060619/408
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7071**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/409
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7072**	N/A	A-ADO-ACRO-060619/410
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7073**	b19-07.html	
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7074**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/412
Use After Free	24-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7075**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/413
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7076		
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7077**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/415
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7078**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/416
Out-of-bounds Write	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7079**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/417
Double Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7080**	b19-07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7081**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/419
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7082**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/420
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7083**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7084**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/422
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7109**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/423
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7110**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/424
Out-of-bounds Write	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7111**	17.html	
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7112**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/426
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7113**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/427
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7114**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7115**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/429
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7116**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/430
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7117**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/431
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7118**	17.html	
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7119**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/433
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7120**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/434
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7121**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7122**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/436
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7123**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/437
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7124**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/438
Improper Restriction of Operations within the	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7125**	17.html	
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7127**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/440
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7128**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/441
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7140**	N/A	A-ADO-ACRO-060619/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7141**	N/A	A-ADO-ACRO-060619/443
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7142**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/444
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7143**	N/A	A-ADO-ACRO-060619/445
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	N/A	A-ADO-ACRO-060619/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7144**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7145**	N/A	A-ADO-ACRO-060619/447
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7758**	N/A	A-ADO-ACRO-060619/448
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and	N/A	A-ADO-ACRO-060619/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7759**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7760**	N/A	A-ADO-ACRO-060619/450
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7761**	N/A	A-ADO-ACRO-060619/451
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7762**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7763**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/453
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7764**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/454
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-7765**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7766**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/456
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7767**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/457
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7768**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7769**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/459
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7770**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/460
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7771**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/461
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	https://helpx.adobe.com/security	A-ADO-ACRO-060619/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7772**	/products/acrobat/apsb19-18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7773**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/463
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7774**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/464
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7775**	18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7776**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/466
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7777**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/467
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability.	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7778**		
N/A	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7779**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/469
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7780**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/470
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7781		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7782**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/472
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7783**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/473
Double Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7784**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/474
Use After Free	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-060619/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7785**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7786**	N/A	A-ADO-ACRO-060619/476
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7787**	N/A	A-ADO-ACRO-060619/477
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7788**	acrobat/apsb19-18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7789**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/479
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7790**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/480
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7791**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7792**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/482
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7793**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/483
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	N/A	A-ADO-ACRO-060619/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2019-7794**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7795**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/485
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7796**	N/A	A-ADO-ACRO-060619/486
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7797**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/487

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
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7798**	N/A	A-ADO-ACRO-060619/488
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7799**	N/A	A-ADO-ACRO-060619/489
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7800**	N/A	A-ADO-ACRO-060619/490
Out-of-	22-05-2019	4.3	Adobe Acrobat and Reader	N/A	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7801**		060619/491
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7802**	N/A	A-ADO-ACRO-060619/492
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7803**	N/A	A-ADO-ACRO-060619/493
Out-of-bounds Write	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7804**	acrobat/apsb19-18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7805**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/495
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7806**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/496
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7807**	b19-18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7808**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/498
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7809**	N/A	A-ADO-ACRO-060619/499
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-	N/A	A-ADO-ACRO-060619/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7810**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7811**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/501
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7812**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/502
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7813		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7814**	N/A	A-ADO-ACRO-060619/504
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20091 and earlier, 2019.010.20091 and earlier, 2017.011.30120 and earlier version, and 2015.006.30475 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7815**	https://helpx.adobe.com/security/products/acrobat/apsb19-13.html	A-ADO-ACRO-060619/505
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7817**	N/A	A-ADO-ACRO-060619/506
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	N/A	A-ADO-ACRO-060619/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7818**		
Incorrect Type Conversion or Cast	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7820**	N/A	A-ADO-ACRO-060619/508
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7821**	N/A	A-ADO-ACRO-060619/509
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	N/A	A-ADO-ACRO-060619/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7822**		
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7823**	N/A	A-ADO-ACRO-060619/511
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7824**	N/A	A-ADO-ACRO-060619/512
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and	N/A	A-ADO-ACRO-060619/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7825**		
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7826**	N/A	A-ADO-ACRO-060619/514
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7827**	N/A	A-ADO-ACRO-060619/515
Improper Restriction of Operations within the	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and	N/A	A-ADO-ACRO-060619/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7828**		
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7829**	N/A	A-ADO-ACRO-060619/517
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7830**	N/A	A-ADO-ACRO-060619/518
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	N/A	A-ADO-ACRO-060619/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7831**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7832**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/520
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7833**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/521
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-7834**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7835**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/523
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7836**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/524
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7841**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
acrobat_reader_dc					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7085**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/526
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7086**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/527
Incorrect Type Conversion or Cast	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7087**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/528
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7088**	b19-17.html	
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7089**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/530
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7018**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/531
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7019**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7020**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/533
Use After Free	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7021**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/534
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7022**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/535
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7023**	07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7024**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/537
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7025**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/538
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7026**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7027**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/540
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7028**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/541
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7029**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/542
Integer Overflow or Wraparound	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an integer overflow vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7030**	07.html	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7031**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/544
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7032**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/545
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7033**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7034**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/547
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7035**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/548
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7036**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/549
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7037**	07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7038**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/551
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7039**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/552
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7040**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	24-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-7041**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/554
NULL Pointer Dereference	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7042**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/555
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7043**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/556
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7044**	b19-07.html	
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7045**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/558
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7046**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/559
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7047		
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7048**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/561
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7049**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/562
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7050**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/563
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7051**	b19-07.html	
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7052**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/565
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7053**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/566
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			. **CVE ID : CVE-2019-7054**		
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7055**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/568
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7056**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/569
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7057**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/570
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7058**	acrobat/apsb19-07.html	
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7059**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/572
Out-of-bounds Write	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7060**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/573
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7061		
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7062**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/575
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7063**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/576
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7064**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/577
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7065**	b19-07.html	
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7066**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/579
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7067**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/580
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7068		
Incorrect Type Conversion or Cast	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7069**	N/A	A-ADO-ACRO-060619/582
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7070**	N/A	A-ADO-ACRO-060619/583
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7071**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/584
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	N/A	A-ADO-ACRO-060619/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7072**		
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7073**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/586
Out-of-bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7074**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/587
Use After Free	24-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7075**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/588

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7076**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/589
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7077**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/590
Use After Free	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7078**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/591
Out-of-bounds Write	24-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-060619/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7079**	b19-07.html	
Double Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7080**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/593
Out-of-bounds Read	24-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7081**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/594
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7082**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7083**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/596
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7084**	https://helpx.adobe.com/security/products/acrobat/apsb19-07.html	A-ADO-ACRO-060619/597
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7109**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/598
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7110**	17.html	
Out-of-bounds Write	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7111**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/600
Use After Free	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7112**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/601
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7113**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7114**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/603
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7115**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/604
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7116**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/605
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7117**	17.html	
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7118**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/607
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7119**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/608
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7120**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7121**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/610
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7122**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/611
Out-of-bounds Read	23-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7123**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/612
Out-of-bounds Write	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7124**	17.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7125**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/614
Out-of-bounds Read	23-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7127**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/615
Incorrect Type Conversion or Cast	23-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and earlier version, and 2015.006.30482 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7128**	https://helpx.adobe.com/security/products/acrobat/apsb19-17.html	A-ADO-ACRO-060619/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7140**	N/A	A-ADO-ACRO-060619/617
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7141**	N/A	A-ADO-ACRO-060619/618
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7142**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/619
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	N/A	A-ADO-ACRO-060619/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7143**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7144**	N/A	A-ADO-ACRO-060619/621
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7145**	N/A	A-ADO-ACRO-060619/622
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier	N/A	A-ADO-ACRO-060619/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7758**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7759**	N/A	A-ADO-ACRO-060619/624
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7760**	N/A	A-ADO-ACRO-060619/625
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free	N/A	A-ADO-ACRO-060619/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7761**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7762**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/627
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7763**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/628
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-7764**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7765**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/630
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7766**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/631
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7767**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7768**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/633
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7769**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/634
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7770**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/635
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	https://helpx.adobe.com/security	A-ADO-ACRO-060619/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7771**	/products/acrobat/apsb19-18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7772**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/637
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7773**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/638
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and	https://helpx.adobe.com/security/products/acrobat/apsb19-	A-ADO-ACRO-060619/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7774**	18.html	
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7775**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/640
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7776**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/641
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability.	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7777**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7778**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/643
N/A	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7779**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/644
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7780		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7781**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/646
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7782**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/647
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7783**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/648
Double Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and	https://helpx.adobe.co	A-ADO-ACRO-060619/649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7784**	m/security /products/ acrobat/aps b19-18.html	
Use After Free	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7785**	N/A	A-ADO-ACRO-060619/650
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7786**	N/A	A-ADO-ACRO-060619/651
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version,	N/A	A-ADO-ACRO-060619/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7787**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7788**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/653
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7789**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/654
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7790**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7791**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/656
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7792**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/657
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2019-7793**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7794**	N/A	A-ADO-ACRO-060619/659
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7795**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/660
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7796**	N/A	A-ADO-ACRO-060619/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7797**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/662
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7798**	N/A	A-ADO-ACRO-060619/663
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7799**	N/A	A-ADO-ACRO-060619/664
Out-of-	22-05-2019	9.3	Adobe Acrobat and Reader	N/A	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7800**		060619/665
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7801**	N/A	A-ADO-ACRO-060619/666
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7802**	N/A	A-ADO-ACRO-060619/667
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	N/A	A-ADO-ACRO-060619/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7803**		
Out-of-bounds Write	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-7804**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/669
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7805**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/670
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060619/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7806**	acrobat/apsb19-18.html	
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7807**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/672
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7808**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/673
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493	N/A	A-ADO-ACRO-060619/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7809**		
Out-of-bounds Read	22-05-2019	4.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7810**	N/A	A-ADO-ACRO-060619/675
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7811**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/676
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2019-7812**		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7813**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/678
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7814**	N/A	A-ADO-ACRO-060619/679
Information Exposure	24-05-2019	7.8	Adobe Acrobat and Reader versions 2019.010.20091 and earlier, 2019.010.20091 and earlier, 2017.011.30120 and earlier version, and 2015.006.30475 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7815**	https://helpx.adobe.com/security/products/acrobat/apsb19-13.html	A-ADO-ACRO-060619/680
Use After	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7817**		060619/681
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7818**	N/A	A-ADO-ACRO-060619/682
Incorrect Type Conversion or Cast	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7820**	N/A	A-ADO-ACRO-060619/683
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and	N/A	A-ADO-ACRO-060619/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7821**		
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7822**	N/A	A-ADO-ACRO-060619/685
Use After Free	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7823**	N/A	A-ADO-ACRO-060619/686
Improper Restriction of Operatio	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and	N/A	A-ADO-ACRO-060619/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ns within the Bounds of a Memory Buffer			earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7824**		
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7825**	N/A	A-ADO-ACRO-060619/688
Out-of-bounds Read	22-05-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7826**	N/A	A-ADO-ACRO-060619/689
Improper Restriction of Operations within the	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and	N/A	A-ADO-ACRO-060619/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7827**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7828**	N/A	A-ADO-ACRO-060619/691
Out-of-bounds Write	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7829**	N/A	A-ADO-ACRO-060619/692
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and	N/A	A-ADO-ACRO-060619/693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7830**		
Use After Free	22-05-2019	9.3	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7831**	N/A	A-ADO-ACRO-060619/694
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7832**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/695
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7833**		
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7834**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/697
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier version, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7835**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/698
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7836		
Out-of-bounds Read	22-05-2019	5	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7841**	https://helpx.adobe.com/security/products/acrobat/apsb19-18.html	A-ADO-ACRO-060619/700
flash_player					
Out-of-bounds Read	24-05-2019	4.3	Flash Player Desktop Runtime versions 32.0.0.114 and earlier, Flash Player for Google Chrome versions 32.0.0.114 and earlier, and Flash Player for Microsoft Edge and Internet Explorer 11 versions 32.0.0.114 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7090**	https://helpx.adobe.com/security/products/flash-player/apsb19-06.html	A-ADO-FLAS-060619/701
Use After Free	23-05-2019	10	Adobe Flash Player versions 32.0.0.156 and earlier, 32.0.0.156 and earlier, and 32.0.0.156 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7096**	https://helpx.adobe.com/security/products/flash-player/apsb19-19.html	A-ADO-FLAS-060619/702
Out-of-bounds Read	23-05-2019	5	Adobe Flash Player versions 32.0.0.156 and earlier, 32.0.0.156 and earlier, and 32.0.0.156 and earlier have an	https://helpx.adobe.com/security/products/f	A-ADO-FLAS-060619/703

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7108**	lash-player/apsb19-19.html	
Use After Free	22-05-2019	9.3	Adobe Flash Player versions 32.0.0.171 and earlier, 32.0.0.171 and earlier, and 32.0.0.171 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7837**	N/A	A-ADO-FLAS-060619/704
flash_player_desktop_runtime					
Out-of-bounds Read	24-05-2019	4.3	Flash Player Desktop Runtime versions 32.0.0.114 and earlier, Flash Player for Google Chrome versions 32.0.0.114 and earlier, and Flash Player for Microsoft Edge and Internet Explorer 11 versions 32.0.0.114 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7090**	https://helpx.adobe.com/security/products/flash-player/apsb19-06.html	A-ADO-FLAS-060619/705
Use After Free	23-05-2019	10	Adobe Flash Player versions 32.0.0.156 and earlier, 32.0.0.156 and earlier, and 32.0.0.156 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7096**	https://helpx.adobe.com/security/products/flash-player/apsb19-19.html	A-ADO-FLAS-060619/706
Out-of-bounds	23-05-2019	5	Adobe Flash Player versions 32.0.0.156 and earlier,	https://helpx.adobe.co	A-ADO-FLAS-060619/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			32.0.0.156 and earlier, and 32.0.0.156 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7108**	m/security/products/flash-player/apsb19-19.html	
Use After Free	22-05-2019	9.3	Adobe Flash Player versions 32.0.0.171 and earlier, 32.0.0.171 and earlier, and 32.0.0.171 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7837**	N/A	A-ADO-FLAS-060619/708
coldfusion					
Deserialization of Untrusted Data	24-05-2019	10	ColdFusion versions Update 1 and earlier, Update 7 and earlier, and Update 15 and earlier have a deserialization of untrusted data vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7091**	https://helpx.adobe.com/security/products/coldfusion/apsb19-10.html	A-ADO-COLD-060619/709
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2019	4.3	ColdFusion versions Update 1 and earlier, Update 7 and earlier, and Update 15 and earlier have a cross site scripting vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-7092**	https://helpx.adobe.com/security/products/coldfusion/apsb19-10.html	A-ADO-COLD-060619/710
Unrestricted	24-05-2019	10	ColdFusion versions Update 2 and earlier, Update 9 and	https://helpx.adobe.co	A-ADO-COLD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Upload of File with Dangerous Type			earlier, and Update 17 and earlier have a file upload restriction bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7816**	m/security/products/coldfusion/apsb19-14.html	060619/711
creative_cloud					
Untrusted Search Path	24-05-2019	6.8	Creative Cloud Desktop Application (installer) versions 4.7.0.400 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-7093**	https://helpx.adobe.com/security/products/creative-cloud/apsb19-11.html	A-ADO-CREA-060619/712
digital_editions					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Digital Editions versions 4.5.10.185749 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7095**	https://helpx.adobe.com/security/products/Digital-Editions/apsb19-16.html	A-ADO-DIGI-060619/713
dreamweaver					
Information Exposure	23-05-2019	5	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack. **CVE ID : CVE-2019-7097**	https://helpx.adobe.com/security/products/dreamweaver/apsb19-21.html	A-ADO-DREA-060619/714
indesign					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-05-2019	10	Adobe InDesign versions 14.0.1 and below have an unsafe hyperlink processing vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7107**	https://helpx.adobe.com/security/products/indesign/apsb19-23.html	A-ADO-INDE-060619/715
experience_manager_forms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-05-2019	4.3	Adobe Experience Manager Forms versions 6.2, 6.3 and 6.4 have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2019-7129**	https://helpx.adobe.com/security/products/aem-forms/apsb19-24.html	A-ADO-EXPE-060619/716
xd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-05-2019	10	Adobe XD versions 16.0 and earlier have a path traversal vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7105**	https://helpx.adobe.com/security/products/xd/apsb19-22.html	A-ADO-XD-060619/717
Improper Limitation of a Pathname to a Restricted Directory	23-05-2019	10	Adobe XD versions 16.0 and earlier have a path traversal vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7106**	https://helpx.adobe.com/security/products/xd/apsb19-22.html	A-ADO-XD-060619/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')					
shockwave_player					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwave Player versions 12.3.4.204 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7098**	https://helpx.adobe.com/security/products/shockwave/apsb19-20.html	A-ADO-SHOC-060619/719
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwave Player versions 12.3.4.204 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7099**	https://helpx.adobe.com/security/products/shockwave/apsb19-20.html	A-ADO-SHOC-060619/720
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwave Player versions 12.3.4.204 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7100**	https://helpx.adobe.com/security/products/shockwave/apsb19-20.html	A-ADO-SHOC-060619/721
Improper Restriction of Operations within the	23-05-2019	10	Adobe Shockwave Player versions 12.3.4.204 and earlier have a memory corruption vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/shockwave/apsb19-	A-ADO-SHOC-060619/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			arbitrary code execution. **CVE ID : CVE-2019-7101**	20.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwave Player versions 12.3.4.204 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7102**	https://helpx.adobe.com/security/products/shockwave/apsb19-20.html	A-ADO-SHOC-060619/723
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwave Player versions 12.3.4.204 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7103**	https://helpx.adobe.com/security/products/shockwave/apsb19-20.html	A-ADO-SHOC-060619/724
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwave Player versions 12.3.4.204 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7104**	https://helpx.adobe.com/security/products/shockwave/apsb19-20.html	A-ADO-SHOC-060619/725
bridge_cc					
Improper Restriction of Operations within	23-05-2019	10	Adobe Bridge CC versions 9.0.2 have a heap overflow vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/bridge/aps	A-ADO-BRID-060619/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
the Bounds of a Memory Buffer			remote code execution. **CVE ID : CVE-2019-7130**	b19-25.html	
Out-of-bounds Write	23-05-2019	9.3	Adobe Bridge CC versions 9.0.2 have an out-of-bounds write vulnerability. Successful exploitation could lead to remote code execution. **CVE ID : CVE-2019-7132**	N/A	A-ADO-BRID-060619/727
Out-of-bounds Read	23-05-2019	4.3	Adobe Bridge CC versions 9.0.2 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7133**	https://helpx.adobe.com/security/products/bridge/apsb19-25.html	A-ADO-BRID-060619/728
Out-of-bounds Read	23-05-2019	4.3	Adobe Bridge CC versions 9.0.2 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7134**	N/A	A-ADO-BRID-060619/729
Out-of-bounds Read	23-05-2019	4.3	Adobe Bridge CC versions 9.0.2 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7135**	N/A	A-ADO-BRID-060619/730
Use After Free	23-05-2019	4.3	Adobe Bridge CC versions 9.0.2 have an use after free vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7136**	N/A	A-ADO-BRID-060619/731
Information	23-05-2019	4.3	Adobe Bridge CC versions 9.0.2 have a memory corruption	N/A	A-ADO-BRID-060619/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7137**		
Out-of-bounds Read	23-05-2019	4.3	Adobe Bridge CC versions 9.0.2 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7138**	N/A	A-ADO-BRID-060619/733
media_encoder					
Use After Free	22-05-2019	6.8	Adobe Media Encoder version 13.0.2 has a use-after-free vulnerability. Successful exploitation could lead to remote code execution. **CVE ID : CVE-2019-7842**	N/A	A-ADO-MEDI-060619/734
Out-of-bounds Read	22-05-2019	4.3	Adobe Media Encoder version 13.0.2 has an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2019-7844**	N/A	A-ADO-MEDI-060619/735
photoshop_cc					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	10	Adobe Photoshop CC 19.1.7 and earlier, and 20.0.2 and earlier have a heap corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7094**	https://helpx.adobe.com/security/products/photoshop/apsb19-15.html	A-ADO-PHOT-060619/736
afian					
filerun					
Improper	30-05-2019	5	FileRun 2019.05.21 allows	N/A	A-AFI-FILE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			images/extjs Directory Listing. **CVE ID : CVE-2019-12457**		060619/737
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-05-2019	5	FileRun 2019.05.21 allows css/ext-ux Directory Listing. **CVE ID : CVE-2019-12458**	N/A	A-AFI-FILE-060619/738
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-05-2019	5	FileRun 2019.05.21 allows customizables/plugins/audio_player Directory Listing. **CVE ID : CVE-2019-12459**	N/A	A-AFI-FILE-060619/739
Apache					
tomcat					
Improper Neutralization of Input During Web Page	28-05-2019	4.3	The SSI printenv command in Apache Tomcat 9.0.0.M1 to 9.0.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 echoes user provided data without escaping and is, therefore, vulnerable to	N/A	A-APA-TOMC-060619/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website. **CVE ID : CVE-2019-0221**		
zookeeper					
N/A	23-05-2019	4.3	An issue is present in Apache ZooKeeper 1.0.0 to 3.4.13 and 3.5.0-alpha to 3.5.4-beta. ZooKeeper?s getACL() command doesn?t check any permission when retrieves the ACLs of the requested node and returns all information contained in the ACL Id field as plaintext string. DigestAuthenticationProvider overloads the Id field with the hash value that is used for user authentication. As a consequence, if Digest Authentication is in use, the unsalted hash value will be disclosed by getACL() request for unauthenticated or unprivileged users. **CVE ID : CVE-2019-0201**	https://zookeeper.apache.org/security.html#CVE-2019-0201	A-APA-ZOOK-060619/741
jspwiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'	20-05-2019	4.3	A carefully crafted malicious attachment could trigger an XSS vulnerability on Apache JSPWiki 2.9.0 to 2.11.0.M3, which could lead to session hijacking. **CVE ID : CVE-2019-10076**	N/A	A-APA-JSPW-060619/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-05-2019	4.3	A carefully crafted InterWiki link could trigger an XSS vulnerability on Apache JSPWiki 2.9.0 to 2.11.0.M3, which could lead to session hijacking. **CVE ID : CVE-2019-10077**	N/A	A-APA-JSPW-060619/743
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-05-2019	4.3	A carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki 2.9.0 to 2.11.0.M3, which could lead to session hijacking. Initial reporting indicated ReferredPagesPlugin, but further analysis showed that multiple plugins were vulnerable. **CVE ID : CVE-2019-10078**	N/A	A-APA-JSPW-060619/744
camel					
Improper Restriction of XML External Entity Reference ('XXE')	28-05-2019	5	Apache Camel prior to 2.24.0 contains an XML external entity injection (XXE) vulnerability (CWE-611) due to using an outdated vulnerable JSON-lib library. This affects only the camel-xmljson component, which was removed. **CVE ID : CVE-2019-0188**	N/A	A-APA-CAME-060619/745
Apachefriends					
xampp					
Improper Neutralization of	16-05-2019	4.3	XAMPP through 5.6.8 allows XSS via the cds-fpdf.php interpret or titel parameter.	N/A	A-APA-XAMP-060619/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			NOTE: This product is discontinued. **CVE ID : CVE-2019-8924**		
applaudsolutions					
applaud_hcm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-05-2019	4.3	Applaud HCM 4.0.42+ uses HTML tag fields for HTML inputs in a form. This leads to an XSS vulnerability with a payload starting with the <iframe./> substring. **CVE ID : CVE-2019-11033**	N/A	A-APP-APPL-060619/747
Artifex					
ghostscript					
N/A	16-05-2019	6.8	It was found that in ghostscript some privileged operators remained accessible from various places after the CVE-2019-6116 fix. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constrains imposed by -dSAFER. Ghostscript versions before 9.27 are vulnerable. **CVE ID : CVE-2019-3839**	N/A	A-ART-GHOS-060619/748
Atlassian					
jira					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	22-05-2019	5	The ManageFilters.jspa resource in Jira before version 7.13.3 and from version 8.0.0 before version 8.1.1 allows remote attackers to enumerate usernames via an incorrect authorisation check. **CVE ID : CVE-2019-3401**	N/A	A-ATL-JIRA-060619/749
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-05-2019	4.3	The ConfigurePortalPages.jspa resource in Jira before version 7.13.3 and from version 8.0.0 before version 8.1.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the searchOwnerUserName parameter. **CVE ID : CVE-2019-3402**	N/A	A-ATL-JIRA-060619/750
Improper Authorization	22-05-2019	5	The /rest/api/2/user/picker rest resource in Jira before version 7.13.3, from version 8.0.0 before version 8.0.4, and from version 8.1.0 before version 8.1.1 allows remote attackers to enumerate usernames via an incorrect authorisation check. **CVE ID : CVE-2019-3403**	N/A	A-ATL-JIRA-060619/751
Improper Access Control	22-05-2019	5	The CachingResourceDownloadRewriteRule class in Jira before version 7.13.4, and from version 8.0.0 before version 8.0.4, and from version 8.1.0 before version 8.1.1 allows remote attackers to access files in the Jira webroot under the META-INF directory via a lax	N/A	A-ATL-JIRA-060619/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			path access check. **CVE ID : CVE-2019-8442**		
Improper Access Control	22-05-2019	6.8	The ViewUpgrades resource in Jira before version 7.13.4, from version 8.0.0 before version 8.0.4, and from version 8.1.0 before version 8.1.1 allows remote attackers who have obtained access to administrator's session to access the ViewUpgrades administrative resource without needing to re-authenticate to pass "WebSudo" through an improper access control vulnerability. **CVE ID : CVE-2019-8443**	N/A	A-ATL-JIRA-060619/753
Atutor					
atutor					
Unrestricted Upload of File with Dangerous Type	17-05-2019	9	ATutor through 2.2.4 is vulnerable to arbitrary file uploads via the mods/_core/backups/upload.php (aka backup) component. This may result in remote command execution. An attacker can use the instructor account to fully compromise the system using a crafted backup ZIP archive. This will allow for PHP files to be written to the web root, and for code to execute on the remote server. **CVE ID : CVE-2019-12170**	N/A	A-ATU-ATUT-060619/754
bacnet_protocol_stack_project					
bacnet_protocol_stack					
Out-of-	30-05-2019	5	BACnet Protocol Stack through	N/A	A-BAC-BACN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			0.8.6 could allow an unauthenticated, remote attacker to cause a denial of service (bacserv daemon crash) because there is an invalid read in bacdcode.c during parsing of alarm tag numbers. **CVE ID : CVE-2019-12480**		060619/755
blogifier					
blogifier					
Improper Input Validation	22-05-2019	7.5	Blogifier 2.3 before 2019-05-11 does not properly restrict APIs, as demonstrated by missing checks for .. in a pathname. **CVE ID : CVE-2019-12277**	N/A	A-BLO-BLOG-060619/756
bluecats					
bc_reveal					
N/A	22-05-2019	4.3	The iOS mobile application BlueCats Reveal before 5.14 stores the username and password in the app cache as base64 encoded strings, i.e. clear text. These persist in the cache even if the user logs out. This can allow an attacker to compromise the affected BlueCats network implementation. The attacker would first need to gain physical control of the iOS device or compromise it with a malicious app. **CVE ID : CVE-2019-5627**	N/A	A-BLU-BC_R-060619/757
blueprism					
robotic_process_automation					
N/A	24-05-2019	6.5	In AutomateAppCore.dll in Blue Prism Robotic Process	N/A	A-BLU-ROBO-060619/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Automation 6.4.0.8445, a vulnerability in access control can be exploited to escalate privileges. The vulnerability allows for abusing the application for fraud or unauthorized access to certain information. The attack requires a valid user account to connect to the Blue Prism server, but the roles associated to this account are not required to have any permissions. First of all, the application files are modified to grant full permissions on the client side. In a test environment (or his own instance of the software) an attacker is able to grant himself full privileges also on the server side. He can then, for instance, create a process with malicious behavior and export it to disk. With the modified client, it is possible to import the exported file as a release and overwrite any existing process in the database. Eventually, the bots execute the malicious process. The server does not check the user's permissions for the aforementioned actions, such that a modification of the client software enables this kind of attack. Possible scenarios may involve changing bank accounts or setting passwords. **CVE ID : CVE-2019-11875**		
BMC					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
patrol_agent					
N/A	20-05-2019	7.5	By default, BMC PATROL Agent through 11.3.01 uses a static encryption key for encrypting/decrypting user credentials sent over the network to managed PATROL Agent services. If an attacker were able to capture this network traffic, they could decrypt these credentials and use them to execute code or escalate privileges on the network. **CVE ID : CVE-2019-8352**	N/A	A-BMC-PATR-060619/759
boostio					
boostnote					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-05-2019	3.5	There is XSS in browser/components/MarkdownPreview.js in BoostIO Boostnote 0.11.15 via a label named flowchart, sequence, gallery, or chart, as demonstrated by a crafted SRC attribute of an IFRAME element, a different vulnerability than CVE-2019-12136. **CVE ID : CVE-2019-12184**	N/A	A-BOO-BOOS-060619/760
bosch					
building_integration_system					
Improper Restriction of Operations within the Bounds	29-05-2019	7.5	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Video Recording Manager (VRM), Video	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-	A-BOS-BUIL-060619/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			Streaming Gateway (VSG), Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The vulnerability potentially allows the unauthorized execution of code in the system via the network interface. **CVE ID : CVE-2019-6957**	2019-0403bt-cve-2019-6957_security_advisory_software_buffer_overflow.pdf	
Improper Access Control	29-05-2019	6.4	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The RCP+ network port allows access without authentication. Adding authentication feature to the respective library fixes the issue. The issue is classified as "CWE-284: Improper Access Control." This vulnerability, for example, allows a potential attacker to delete video or read video data. **CVE ID : CVE-2019-6958**	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-0404bt-cve-2019-6958_security_advisory_improper_access_control.pdf	A-BOS-BUIL-060619/762
bosch_video_management_system					
Improper Restriction of	29-05-2019	7.5	A recently discovered security vulnerability affects all Bosch Video Management System	https://media.boschsecurity.com/	A-BOS-BOSC-060619/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			(BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Video Recording Manager (VRM), Video Streaming Gateway (VSG), Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The vulnerability potentially allows the unauthorized execution of code in the system via the network interface. **CVE ID : CVE-2019-6957**	fs/media/pb/security_advisories/bosch-2019-0403bt-cve-2019-6957_security_advisory_software_buffer_overflow.pdf	
Improper Access Control	29-05-2019	6.4	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The RCP+ network port allows access without authentication. Adding authentication feature to the respective library fixes the issue. The issue is classified as "CWE-284: Improper Access Control." This vulnerability, for example, allows a potential attacker to delete video or read video data. **CVE ID : CVE-2019-6958**	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-0404bt-cve-2019-6958_security_advisory_improper_access_control.pdf	A-BOS-BOSC-060619/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buildbot					
buildbot					
Improper Authentication	23-05-2019	5	Buildbot before 1.8.2 and 2.x before 2.3.1 accepts a user-submitted authorization token from OAuth and uses it to authenticate a user. If an attacker has a token allowing them to read the user details of a victim, they can login as the victim. **CVE ID : CVE-2019-12300**	N/A	A-BUI-BUIL-060619/765
CA					
risk_authentication					
Information Exposure	28-05-2019	4	A UI redress vulnerability in the administrative user interface of CA Technologies CA Strong Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 7.1.x and CA Risk Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 3.1.x may allow a remote attacker to gain sensitive information in some cases. **CVE ID : CVE-2019-7393**	https://support.ca.com/us/product-content/recommended-reading/security-notices/CA20190523-01--security-notice-for-ca-risk-authentication-and-ca-strong-authentication.html	A-CA-RISK-060619/766
N/A	28-05-2019	6.5	A privilege escalation vulnerability in the administrative user interface of CA Technologies CA Strong Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 7.1.x and CA Risk	https://support.ca.com/us/product-content/recommended-	A-CA-RISK-060619/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 3.1.x allows an authenticated attacker to gain additional privileges in some cases where an account has customized and limited privileges. **CVE ID : CVE-2019-7394**	reading/security-notices/CA20190523-01--security-notice-for-ca-risk-authentication-and-ca-strong-authentication.html	
strong_authentication					
Information Exposure	28-05-2019	4	A UI redress vulnerability in the administrative user interface of CA Technologies CA Strong Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 7.1.x and CA Risk Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 3.1.x may allow a remote attacker to gain sensitive information in some cases. **CVE ID : CVE-2019-7393**	https://support.ca.com/us/product-content/recommended-reading/security-notices/CA20190523-01--security-notice-for-ca-risk-authentication-and-ca-strong-authentication.html	A-CA-STRO-060619/768
N/A	28-05-2019	6.5	A privilege escalation vulnerability in the administrative user interface of CA Technologies CA Strong Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 7.1.x and CA Risk Authentication 9.0.x, 8.2.x,	https://support.ca.com/us/product-content/recommended-reading/sec	A-CA-STRO-060619/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.1.x, 8.0.x, 3.1.x allows an authenticated attacker to gain additional privileges in some cases where an account has customized and limited privileges. **CVE ID : CVE-2019-7394**	urity-notices/CA20190523-01--security-notice-for-ca-risk-authentication-and-ca-strong-authentication.html	
carts.guru					
carts_guru					
Deserialization of Untrusted Data	20-05-2019	7.5	The Carts Guru plugin 1.4.5 for WordPress allows Insecure Deserialization via a cartsguru-source cookie to classes/wc-cartsguru-event-handler.php. **CVE ID : CVE-2019-12241**	N/A	A-CAR-CART-060619/770
centos-webpanel					
centos_web_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2019	3.5	XSS was discovered in CentOS-WebPanel.com (aka CWP) CentOS Web Panel through 0.9.8.747 via the testacc/fileManager2.php fm_current_dir or filename parameter. **CVE ID : CVE-2019-12190**	N/A	A-CEN-CENT-060619/771
Citrix					
receiver					
Improper Access Control	22-05-2019	7.5	Citrix Workspace App before 1904 for Windows has Incorrect Access Control.	N/A	A-CIT-RECE-060619/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11634		
commsy					
commsy					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-05-2019	5	CommSy through 8.6.5 has SQL Injection via the cid parameter. This is fixed in 9.2. **CVE ID : CVE-2019-11880**	N/A	A-COM-COMM-060619/773
computrols					
computrols_building_automation_software					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-05-2019	4.3	Computrols CBAS 18.0.0 allows Unauthenticated Reflected Cross-Site Scripting vulnerabilities in the login page and password reset page via the username GET parameter. **CVE ID : CVE-2019-10846**	N/A	A-COM-COMP-060619/774
Cross-Site Request Forgery (CSRF)	24-05-2019	6.8	Computrols CBAS 18.0.0 allows Cross-Site Request Forgery. **CVE ID : CVE-2019-10847**	N/A	A-COM-COMP-060619/775
Information Exposure	24-05-2019	5	Computrols CBAS 18.0.0 allows Username Enumeration. **CVE ID : CVE-2019-10848**	N/A	A-COM-COMP-060619/776
Information Exposure	23-05-2019	5	Computrols CBAS 18.0.0 allows unprotected Subversion (SVN) directory / source code	N/A	A-COM-COMP-060619/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure. **CVE ID : CVE-2019-10849**		
Use of Hard-coded Credentials	23-05-2019	10	Computrols CBAS 18.0.0 has Default Credentials. **CVE ID : CVE-2019-10850**	N/A	A-COM-COMP-060619/778
N/A	23-05-2019	4	Computrols CBAS 18.0.0 has hard-coded encryption keys. **CVE ID : CVE-2019-10851**	N/A	A-COM-COMP-060619/779
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-05-2019	6.5	Computrols CBAS 18.0.0 allows Authenticated Blind SQL Injection via the id GET parameter, as demonstrated by the index.php?m=servers&a=start_pulling&id= substring. **CVE ID : CVE-2019-10852**	N/A	A-COM-COMP-060619/780
Improper Authentication	23-05-2019	8.3	Computrols CBAS 18.0.0 allows Authentication Bypass. **CVE ID : CVE-2019-10853**	N/A	A-COM-COMP-060619/781
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-05-2019	9	Computrols CBAS 18.0.0 allows Authenticated Command Injection. **CVE ID : CVE-2019-10854**	N/A	A-COM-COMP-060619/782
Information	23-05-2019	5	Computrols CBAS 18.0.0 mishandles password hashes.	N/A	A-COM-COMP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			The approach is MD5 with a pw prefix, e.g., if the password is admin, it will calculate the MD5 hash of pwadmin and store it in a MySQL database. **CVE ID : CVE-2019-10855**		060619/783
create-sd					
create_sd					
Improper Access Control	17-05-2019	5.8	CREATE SD official App for Android version 1.0.2 and earlier allows remote attackers to bypass access restriction to lead a user to access an arbitrary website via vulnerable application and conduct phishing attacks. **CVE ID : CVE-2019-5955**	N/A	A-CRE-CREA-060619/784
Cybozu					
garoon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	4.3	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.6.3 allows remote attackers to inject arbitrary web script or HTML via Customize Item function. **CVE ID : CVE-2019-5928**	N/A	A-CYB-GARO-060619/785
Improper Neutralization of Input During Web Page Generation ('Cross-	17-05-2019	4.3	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.6.3 allows remote attackers to inject arbitrary web script or HTML via the application 'Memo'. **CVE ID : CVE-2019-5929**	N/A	A-CYB-GARO-060619/786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
site Scripting')					
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 to 4.6.3 allows remote attackers to bypass access restriction to browse unauthorized pages via the application 'Management of Basic System'. **CVE ID : CVE-2019-5930**	N/A	A-CYB-GARO-060619/787
Improper Input Validation	17-05-2019	5.5	Cybozu Garoon 4.0.0 to 4.6.3 allows authenticated attackers to alter the information with privileges invoking the installer via unspecified vectors. **CVE ID : CVE-2019-5931**	N/A	A-CYB-GARO-060619/788
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	3.5	Cross-site scripting vulnerability in Cybozu Garoon 4.6.0 to 4.6.3 allows remote authenticated attackers to inject arbitrary web script or HTML via the application 'Portal'. **CVE ID : CVE-2019-5932**	N/A	A-CYB-GARO-060619/789
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 to 4.10.0 allows remote authenticated attackers to bypass access restriction to view the Bulletin Board without view privileges via the application 'Bulletin'. **CVE ID : CVE-2019-5933**	N/A	A-CYB-GARO-060619/790
Improper Neutralization of Special Elements	17-05-2019	6.5	SQL injection vulnerability in the Cybozu Garoon 4.0.0 to 4.10.0 allows attacker with administrator rights to execute arbitrary SQL commands via	N/A	A-CYB-GARO-060619/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			the Log Search function of application 'logging'. **CVE ID : CVE-2019-5934**		
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to bypass access restriction to change user information without access privileges via the Item function of User Information. **CVE ID : CVE-2019-5935**	N/A	A-CYB-GARO-060619/792
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-05-2019	5.5	Directory traversal vulnerability in Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to obtain files without access privileges via the application 'Work Flow'. **CVE ID : CVE-2019-5936**	N/A	A-CYB-GARO-060619/793
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	3.5	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to inject arbitrary web script or HTML via the user information. **CVE ID : CVE-2019-5937**	N/A	A-CYB-GARO-060619/794
Improper Neutralization of Input	17-05-2019	4.3	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.1 allows remote attackers to inject arbitrary	N/A	A-CYB-GARO-060619/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			web script or HTML via the application 'Mail'. **CVE ID : CVE-2019-5938**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	4.3	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.1 allows remote attackers to inject arbitrary web script or HTML via the application 'Portal'. **CVE ID : CVE-2019-5939**	N/A	A-CYB-GARO-060619/796
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	4.3	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.1 allows remote attackers to inject arbitrary web script or HTML via the application 'Scheduler'. **CVE ID : CVE-2019-5940**	N/A	A-CYB-GARO-060619/797
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to bypass access restriction alter the Report without access privileges via the application 'Multi Report'. **CVE ID : CVE-2019-5941**	N/A	A-CYB-GARO-060619/798
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to bypass access restriction to obtain files	N/A	A-CYB-GARO-060619/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without access privileges via the Multiple Files Download function of application 'Cabinet'. **CVE ID : CVE-2019-5942**		
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to bypass access restriction to view the information without view privileges via the application 'Bulletin' and the application 'Cabinet'. **CVE ID : CVE-2019-5943**	N/A	A-CYB-GARO-060619/800
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 to 4.10.1 allows remote authenticated attackers to bypass access restriction alter the contents of application 'Address' without modify privileges via the application 'Address'. **CVE ID : CVE-2019-5944**	N/A	A-CYB-GARO-060619/801
N/A	17-05-2019	5	Cybozu Garoon 4.2.4 to 4.10.1 allow remote attackers to obtain the users' credential information via the authentication of Cybozu Garoon. **CVE ID : CVE-2019-5945**	N/A	A-CYB-GARO-060619/802
URL Redirection to Untrusted Site ('Open Redirect')	17-05-2019	5.8	Open redirect vulnerability in Cybozu Garoon 4.2.4 to 4.10.1 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the Login Screen. **CVE ID : CVE-2019-5946**	N/A	A-CYB-GARO-060619/803
Improper Neutraliz	17-05-2019	3.5	Cross-site scripting vulnerability in Cybozu Garoon	N/A	A-CYB-GARO-060619/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			4.6.0 to 4.10.1 allows remote authenticated attackers to inject arbitrary web script or HTML via the application 'Cabinet'. **CVE ID : CVE-2019-5947**		
deltek					
maconomy					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-05-2019	7.5	Deltek Maconomy 2.2.5 is prone to local file inclusion via absolute path traversal in the WS.macx1.W_MCS/ PATH_INFO, as demonstrated by a cgi-bin/Maconomy/MaconomyWS.macx1.W_MCS//etc/passwd URI. **CVE ID : CVE-2019-12314**	N/A	A-DEL-MACO-060619/805
digitaldruid					
hoteldruid					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	4.3	HotelDruid 2.3.0 has XSS affecting the nsextt, cambia1, mese_fine, origine, and anno parameters in creaprezzi.php, tabella3.php, personalizza.php, and visualizza_tabelle.php. **CVE ID : CVE-2019-8937**	N/A	A-DIG-HOTE-060619/806
dollarshaveclub					
shave					
Improper	24-05-2019	4.3	XSS exists in Shave before 2.5.3	N/A	A-DOL-SHAV-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			because output encoding is mishandled during the overwrite of an HTML element. **CVE ID : CVE-2019-12313**		060619/807
Dotcms					
dotcms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-05-2019	4	dotCMS before 5.1.0 has a path traversal vulnerability exploitable by an administrator to create files. The vulnerability is caused by the insecure extraction of a ZIP archive. **CVE ID : CVE-2019-12309**	N/A	A-DOT-DOTC-060619/808
Drupal					
drupal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-05-2019	3.5	In Symfony before 2.7.51, 2.8.x before 2.8.50, 3.x before 3.4.26, 4.x before 4.1.12, and 4.2.x before 4.2.7, validation messages are not escaped, which can lead to XSS when user input is included. This is related to symfony/framework-bundle. **CVE ID : CVE-2019-10909**	N/A	A-DRU-DRUP-060619/809
Improper Neutralization of	24-05-2019	4.3	In PrestaShop 1.7.5.2, the shop_country parameter in the install/index.php installation	N/A	A-DRU-DRUP-060619/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			script/component is affected by Reflected XSS. Exploitation by a malicious actor requires the user to follow the initial stages of the setup (accepting terms and conditions) before executing the malicious link. **CVE ID : CVE-2019-11876**		
dynmap_project					
dynmap					
Improper Access Control	28-05-2019	5	In Webbukkit Dynmap 3.0-beta-3, with Spigot 1.13.2, due to a missing login check in servlet/MapStorageHandler.java, an attacker can see a map image without login despite an enabled login-required setting. **CVE ID : CVE-2019-12395**	N/A	A-DYN-DYNM-060619/811
Eaton					
halo_home					
N/A	22-05-2019	4.3	The Android mobile application Halo Home before 1.11.0 stores OAuth authentication and refresh access tokens in a clear text file. This file persists until the user logs out of the application and reboots the device. This vulnerability can allow an attacker to impersonate the legitimate user by reusing the stored OAuth token, thus allowing them to view and change the user's personal information stored in the backend cloud service. The attacker would first need to gain physical control of the Android device or compromise	N/A	A-EAT-HALO-060619/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it with a malicious app. **CVE ID : CVE-2019-5625**		
eficode					
influxdb					
N/A	31-05-2019	4	Jenkins InfluxDB Plugin 1.21 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10329**	N/A	A-EFI-INFL-060619/813
elabftw					
elabftw					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-05-2019	9	eLabFTW 1.8.5 is vulnerable to arbitrary file uploads via the /app/controllers/EntityController.php component. This may result in remote command execution. An attacker can use a user account to fully compromise the system using a POST request. This will allow for PHP files to be written to the web root, and for code to execute on the remote server. **CVE ID : CVE-2019-12185**	N/A	A-ELA-ELAB-060619/814
Enigmail					
enigmail					
Improper Verification of Cryptographic Signature	21-05-2019	5	Enigmail before 2.0.11 allows PGP signature spoofing: for an inline PGP message, an attacker can cause the product to display a "correctly signed" message indication, but display different unauthenticated text. **CVE ID : CVE-2019-12269**	N/A	A-ENI-ENIG-060619/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
falco					
falco					
Use After Free	17-05-2019	2.1	An issue was discovered in Falco through 0.14.0. A missing indicator for insufficient resources allows local users to bypass the detection engine. **CVE ID : CVE-2019-8339**	N/A	A-FAL-FALC-060619/816
Fasterxml					
jackson-databind					
Information Exposure	17-05-2019	5	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint, the service has the mysql-connector-java jar (8.0.14 or earlier) in the classpath, and an attacker can host a crafted MySQL server reachable by the victim, an attacker can send a crafted JSON message that allows them to read arbitrary local files on the server. This occurs because of missing com.mysql.cj.jdbc.admin.MiniAdmin validation. **CVE ID : CVE-2019-12086**	N/A	A-FAS-JACK-060619/817
firejail_project					
firejail					
Improper Input Validation	31-05-2019	9.3	Firejail before 0.9.60 allows truncation (resizing to length 0) of the firejail binary on the host by running exploit code inside a firejail sandbox and	N/A	A-FIR-FIRE-060619/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			having the sandbox terminated. To succeed, certain conditions need to be fulfilled: The jail (with the exploit code inside) needs to be started as root, and it also needs to be terminated as root from the host (either by stopping it ungracefully (e.g., SIGKILL), or by using the --shutdown control command). This is similar to CVE-2019-5736. **CVE ID : CVE-2019-12499**		
Fortinet					
forticlient					
Untrusted Search Path	28-05-2019	9.3	An Unsafe Search Path vulnerability in FortiClient Online Installer (Windows version before 6.0.6) may allow an unauthenticated, remote attacker with control over the directory in which FortiClientOnlineInstaller.exe resides to execute arbitrary code on the system via uploading malicious .dll files in that directory. **CVE ID : CVE-2019-5589**	https://fortiguard.com/advisory/FG-IR-19-060	A-FOR-FORT-060619/819
Freedesktop					
poppler					
Out-of-bounds Read	23-05-2019	6.8	In Poppler through 0.76.1, there is a heap-based buffer over-read in JPXStream::init in JPEG2000Stream.cc via data with inconsistent heights or widths. **CVE ID : CVE-2019-12293**	N/A	A-FRE-POPP-060619/820
freeimage_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
freeimage					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-05-2019	5	When FreeImage 3.18.0 reads a tiff file, it will be handed to the Load function of the PluginTIFF.cpp file, but a memcpy occurs in which the destination address and the size of the copied data are not considered, resulting in a heap overflow. **CVE ID : CVE-2019-12211**	N/A	A-FRE-FREE-060619/821
Uncontrolled Resource Consumption	20-05-2019	5	When FreeImage 3.18.0 reads a special JXR file, the StreamCalcIFDSize function of JXRMeta.c repeatedly calls itself due to improper processing of the file, eventually causing stack exhaustion. An attacker can achieve a remote denial of service attack by sending a specially constructed file. **CVE ID : CVE-2019-12212**	N/A	A-FRE-FREE-060619/822
Uncontrolled Resource Consumption	20-05-2019	4.3	When FreeImage 3.18.0 reads a special TIFF file, the TIFFReadDirectory function in PluginTIFF.cpp always returns 1, leading to stack exhaustion. **CVE ID : CVE-2019-12213**	N/A	A-FRE-FREE-060619/823
Out-of-bounds Read	20-05-2019	5	In FreeImage 3.18.0, an out-of-bounds access occurs because of mishandling of the OpenJPEG j2k_read_ppm_v3 function in j2k.c. The value of l_N_ppm comes from the file read in, and the code does not consider that l_N_ppm may be greater than the size of p_header_data. **CVE ID : CVE-2019-12214**	N/A	A-FRE-FREE-060619/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Freeradius					
freeradius					
N/A	24-05-2019	6.9	It was discovered freeradius up to and including version 3.0.19 does not correctly configure logrotate, allowing a local attacker who already has control of the radiusd user to escalate his privileges to root, by tricking logrotate into writing a radiusd-writable file to a directory normally inaccessible by the radiusd user. **CVE ID : CVE-2019-10143**	https://github.com/FreeRADIUS/freeradius-server/pull/2666	A-FRE-FREE-060619/825
F-secure					
psb_workstation_security					
N/A	17-05-2019	6.8	In the F-Secure installer in F-Secure SAFE for Windows before 17.6, F-Secure Internet Security before 17.6, F-Secure Anti-Virus before 17.6, F-Secure Client Security Standard and Premium before 14.10, F-Secure PSB Workstation Security before 12.01, and F-Secure Computer Protection Standard and Premium before 19.3, a local user can escalate their privileges through a DLL hijacking attack against the installer. The installer writes the file rm.exe to C:\Windows\Temp and then executes it. The rm.exe process then attempts to load several DLLs from its current directory. Non-admin users are able to write to this folder, so an	https://www.f-secure.com/en/web/labs_global/fsc-2019-2	A-F-S-PSB_-060619/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can create a malicious C:\Windows\Temp\OLEACC.dll file. When an admin runs the installer, rm.exe will execute the attacker's DLL in an elevated security context. **CVE ID : CVE-2019-11644**		
gatship					
web_module					
Information Exposure	17-05-2019	5	GAT-Ship Web Module through 1.30 allows remote attackers to obtain potentially sensitive information via {} in a ws/gatshipWs.asmx/SqlVersion request. **CVE ID : CVE-2019-12163**	N/A	A-GAT-WEB_-060619/827
getbukkit					
spigot					
Improper Access Control	28-05-2019	5	In Webbukkit Dynmap 3.0-beta-3, with Spigot 1.13.2, due to a missing login check in servlet/MapStorageHandler.java, an attacker can see a map image without login despite an enabled login-required setting. **CVE ID : CVE-2019-12395**	N/A	A-GET-SPIG-060619/828
Get-simple					
getsimple_cms					
N/A	22-05-2019	5	An issue was discovered in GetSimple CMS through 3.3.15. insufficient input sanitation in the theme-edit.php file allows upload of files with arbitrary content (PHP code, for example). This vulnerability is triggered by an authenticated user; however, authentication	N/A	A-GET-GETS-060619/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be bypassed. According to the official documentation for installation step 10, an admin is required to upload all the files, including the .htaccess files, and run a health check. However, what is overlooked is that the Apache HTTP Server by default no longer enables the AllowOverride directive, leading to data/users/admin.xml password exposure. The passwords are hashed but this can be bypassed by starting with the data/other/authorization.xml API key. This allows one to target the session state, since they decided to roll their own implementation. The cookie_name is crafted information that can be leaked from the frontend (site name and version). If a someone leaks the API key and the admin username, then they can bypass authentication. To do so, they need to supply a cookie based on an SHA-1 computation of this known information. The vulnerability exists in the admin/theme-edit.php file. This file checks for forms submissions via POST requests, and for the csrf nonce. If the nonce sent is correct, then the file provided by the user is uploaded. There is a path traversal allowing write access outside the jailed		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			themes directory root. Exploiting the traversal is not necessary because the .htaccess file is ignored. A contributing factor is that there isn't another check on the extension before saving the file, with the assumption that the parameter content is safe. This allows the creation of web accessible and executable files with arbitrary content. **CVE ID : CVE-2019-11231**		
gitea					
gitea					
Improper Access Control	31-05-2019	5	Jenkins Gitea Plugin 1.1.1 and earlier did not implement trusted revisions, allowing attackers without commit access to the Git repo to change Jenkinsfiles even if Jenkins is configured to consider them to be untrusted. **CVE ID : CVE-2019-10330**	N/A	A-GIT-GITE-060619/830
Gitlab					
gitlab					
N/A	16-05-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The construction of the HMAC key was insecurely derived. **CVE ID : CVE-2019-10112**	N/A	A-GIT-GITL-060619/831
Uncontrolled Resource Consump	16-05-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and	N/A	A-GIT-GITL-060619/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tion			11.9.x before 11.9.2. Making concurrent GET /api/v4/projects/<id>/languages requests may allow Uncontrolled Resource Consumption. **CVE ID : CVE-2019-10113**		
Information Exposure	16-05-2019	5	An Information Exposure issue (issue 2 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. During the OAuth authentication process, the application attempts to validate a parameter in an insecure way, potentially exposing data. **CVE ID : CVE-2019-10114**	N/A	A-GIT-GITL-060619/833
N/A	16-05-2019	4	An Insecure Permissions issue (issue 2 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The GitLab Releases feature could allow guest users access to private information like release details and code information. **CVE ID : CVE-2019-10115**	N/A	A-GIT-GITL-060619/834
N/A	16-05-2019	4	An Insecure Permissions issue (issue 3 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. Guests of a project were allowed to see Related Branches created for an issue.	N/A	A-GIT-GITL-060619/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10116		
URL Redirection to Untrusted Site ('Open Redirect')	16-05-2019	5.8	An Open Redirect issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. A redirect is triggered after successful authentication within the Oauth/:GeoAuthController for the secondary Geo node. **CVE ID : CVE-2019-10117**	N/A	A-GIT-GITL-060619/836
Improper Access Control	17-05-2019	6.4	An Incorrect Access Control issue was discovered in GitLab Community and Enterprise Edition 6.0 and later but before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. The issue comments feature could allow a user to comment on an issue which they shouldn't be allowed to. **CVE ID : CVE-2019-5883**	N/A	A-GIT-GITL-060619/837
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-05-2019	5	An Improper Input Validation issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It was possible to use the profile name to inject a potentially malicious link into notification emails. **CVE ID : CVE-2019-6781**	N/A	A-GIT-GITL-060619/838
Improper Access Control	17-05-2019	4	An Incorrect Access Control issue was discovered in GitLab Community and Enterprise	N/A	A-GIT-GITL-060619/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. The GitLab API allowed project Maintainers and Owners to view the trigger tokens of other project users. **CVE ID : CVE-2019-6787**		
Improper Access Control	17-05-2019	4	An Incorrect Access Control (issue 2 of 3) issue was discovered in GitLab Community and Enterprise Edition 8.14 and later but before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. Guest users were able to view the list of a group's merge requests. **CVE ID : CVE-2019-6790**	N/A	A-GIT-GITL-060619/840
Information Exposure	17-05-2019	5	An information disclosure issue was discovered in GitLab Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. The GitHub token used in CI/CD for External Repos was being leaked to project maintainers in the UI. **CVE ID : CVE-2019-6797**	N/A	A-GIT-GITL-060619/841
Improper Access Control	17-05-2019	6.4	An Incorrect Access Control issue was discovered in GitLab Community and Enterprise Edition 11.7.x before 11.7.4. GitLab Releases were vulnerable to an authorization issue that allowed users to view confidential issue and merge request titles of other projects. **CVE ID : CVE-2019-7353**	N/A	A-GIT-GITL-060619/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	29-05-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x before 11.5.10, 11.6.x before 11.6.8, and 11.7.x before 11.7.3. It has Incorrect Access Control, **CVE ID : CVE-2019-7549**	N/A	A-GIT-GITL-060619/843
Uncontrolled Resource Consumption	29-05-2019	7.8	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Uncontrolled Resource Consumption (issue 2 of 2). **CVE ID : CVE-2019-9177**	N/A	A-GIT-GITL-060619/844
Improper Access Control	29-05-2019	7.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 1 of 5). **CVE ID : CVE-2019-9218**	N/A	A-GIT-GITL-060619/845
Improper Input Validation	29-05-2019	2.1	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 3 of 5). **CVE ID : CVE-2019-9221**	N/A	A-GIT-GITL-060619/846
N/A	29-05-2019	7.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions.	N/A	A-GIT-GITL-060619/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9485		
Improper Access Control	29-05-2019	7.5	An issue was discovered in GitLab Community and Enterprise Edition 10.x (starting from 10.8) and 11.x before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control. **CVE ID : CVE-2019-9732**	N/A	A-GIT-GITL-060619/848
Information Exposure	29-05-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.7.7 and 11.8.x before 11.8.3. It allows Information Disclosure. **CVE ID : CVE-2019-9866**	N/A	A-GIT-GITL-060619/849
glyphandcog					
xpdfreader					
Out-of-bounds Read	27-05-2019	5.8	A stack-based buffer over-read exists in FoFiTrueType::dumpString in fofi/FoFiTrueType.cc in Xpdf 4.01.01. It can, for example, be triggered by sending crafted TrueType data in a PDF document to the pdftops tool. It might allow an attacker to cause Denial of Service or leak memory data into dump content. **CVE ID : CVE-2019-12360**	N/A	A-GLY-XPDF-060619/850
Out-of-bounds Read	30-05-2019	5.8	A stack-based buffer over-read exists in PostScriptFunction::transform in Function.cc in Xpdf 4.01.01 because GfxSeparationColorSpace and GfxDeviceNColorSpace	N/A	A-GLY-XPDF-060619/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mishandle tint transform functions. It can, for example, be triggered by sending a crafted PDF document to the pdftops tool. It might allow an attacker to cause Denial of Service or leak memory data. **CVE ID : CVE-2019-12493**		
Gnome					
gvfs					
N/A	29-05-2019	7.5	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c mishandles file ownership because setfsuid is not used. **CVE ID : CVE-2019-12447**	N/A	A-GNO-GVFS-060619/852
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-05-2019	6.8	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c has race conditions because the admin backend doesn't implement query_info_on_read/write. **CVE ID : CVE-2019-12448**	N/A	A-GNO-GVFS-060619/853
N/A	29-05-2019	10	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c mishandles a file's user and group ownership during move (and copy with G_FILE_COPY_ALL_METADATA) operations from admin:// to	N/A	A-GNO-GVFS-060619/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file:// URIs, because root privileges are unavailable. **CVE ID : CVE-2019-12449**		
glib					
N/A	29-05-2019	7.5	file_copy_fallback in gio/gfile.c in GNOME GLib 2.15.0 through 2.61.1 does not properly restrict file permissions while a copy operation is in progress. Instead, default permissions are used. **CVE ID : CVE-2019-12450**	N/A	A-GNO-GLIB-060619/855
GNU					
wget					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.5	Buffer overflow in GNU Wget 1.20.1 and earlier allows remote attackers to cause a denial-of-service (DoS) or may execute an arbitrary code via unspecified vectors. **CVE ID : CVE-2019-5953**	N/A	A-GNU-WGET-060619/856
gohttp_project					
gohttp					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.5	GoHTTP through 2017-07-25 has a GetExtension heap-based buffer overflow via a long extension. **CVE ID : CVE-2019-12158**	N/A	A-GOH-GOHT-060619/857
Out-of-bounds	17-05-2019	5	GoHTTP through 2017-07-25 has a stack-based buffer over-	N/A	A-GOH-GOHT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			read in the scan function (when called from getRequestType) via a long URL. **CVE ID : CVE-2019-12159**		060619/858
Use After Free	17-05-2019	7.5	GoHTTP through 2017-07-25 has a sendHeader use-after-free. **CVE ID : CVE-2019-12160**	N/A	A-GOH-GOHT-060619/859
Out-of-bounds Read	20-05-2019	5	In GoHttp through 2017-07-25, there is a stack-based buffer over-read via a long User-Agent header. **CVE ID : CVE-2019-12198**	N/A	A-GOH-GOHT-060619/860
Golang					
crypto					
N/A	22-05-2019	4.3	A message-forgery issue was discovered in crypto/openpgp/clearsign/clearsign.go in supplementary Go cryptography libraries 2019-03-25. According to the OpenPGP Message Format specification in RFC 4880 chapter 7, a cleartext signed message can contain one or more optional "Hash" Armor Headers. The "Hash" Armor Header specifies the message digest algorithm(s) used for the signature. However, the Go clearsign package ignores the value of this header, which allows an attacker to spoof it. Consequently, an attacker can lead a victim to believe the signature was generated using a different message digest algorithm than what was actually used. Moreover, since	N/A	A-GOL-CRYP-060619/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the library skips Armor Header parsing in general, an attacker can not only embed arbitrary Armor Headers, but also prepend arbitrary text to cleartext messages without invalidating the signatures. **CVE ID : CVE-2019-11841**		
Google					
chrome					
Use After Free	23-05-2019	9.3	Use-after-garbage-collection in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2019-5787**	N/A	A-GOO-CHRO-060619/862
Integer Overflow or Wraparound	23-05-2019	9.3	An integer overflow that leads to a use-after-free in Blink Storage in Google Chrome on Linux prior to 73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. **CVE ID : CVE-2019-5788**	N/A	A-GOO-CHRO-060619/863
Integer Overflow or Wraparound	23-05-2019	9.3	An integer overflow that leads to a use-after-free in WebMIDI in Google Chrome on Windows prior to 73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. **CVE ID : CVE-2019-5789**	N/A	A-GOO-CHRO-060619/864
Integer Overflow or	23-05-2019	6.8	An integer overflow leading to an incorrect capacity of a buffer in JavaScript in Google Chrome	N/A	A-GOO-CHRO-060619/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			prior to 73.0.3683.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. **CVE ID : CVE-2019-5790**		
Incorrect Type Conversion or Cast	23-05-2019	6.8	Inappropriate optimization in V8 in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. **CVE ID : CVE-2019-5791**	N/A	A-GOO-CHRO-060619/866
Integer Overflow or Wraparound	23-05-2019	6.8	Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file. **CVE ID : CVE-2019-5792**	N/A	A-GOO-CHRO-060619/867
Improper Input Validation	23-05-2019	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to initiate the extensions installation user interface via a crafted HTML page. **CVE ID : CVE-2019-5793**	N/A	A-GOO-CHRO-060619/868
Improper Input Validation	23-05-2019	4.3	Incorrect handling of cancelled requests in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page. **CVE ID : CVE-2019-5794**	N/A	A-GOO-CHRO-060619/869
Integer Overflow or	23-05-2019	6.8	Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote	N/A	A-GOO-CHRO-060619/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			attacker to potentially perform out of bounds memory access via a crafted PDF file. **CVE ID : CVE-2019-5795**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	23-05-2019	5.1	Data race in extensions guest view in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2019-5796**	N/A	A-GOO-CHRO-060619/871
Out-of-bounds Read	23-05-2019	4.3	Lack of correct bounds checking in Skia in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. **CVE ID : CVE-2019-5798**	N/A	A-GOO-CHRO-060619/872
Improper Input Validation	23-05-2019	4.3	Incorrect inheritance of a new document's policy in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2019-5799**	N/A	A-GOO-CHRO-060619/873
Improper Input Validation	23-05-2019	4.3	Insufficient policy enforcement in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.	N/A	A-GOO-CHRO-060619/874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5800		
Improper Input Validation	23-05-2019	4.3	Incorrect eliding of URLs in Omnibox in Google Chrome on iOS prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page. **CVE ID : CVE-2019-5801**	N/A	A-GOO-CHRO-060619/875
Improper Input Validation	23-05-2019	4.3	Incorrect handling of download origins in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page. **CVE ID : CVE-2019-5802**	N/A	A-GOO-CHRO-060619/876
Improper Input Validation	23-05-2019	4.3	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2019-5803**	N/A	A-GOO-CHRO-060619/877
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-05-2019	2.1	Incorrect command line processing in Chrome in Google Chrome prior to 73.0.3683.75 allowed a local attacker to perform domain spoofing via a crafted domain name. **CVE ID : CVE-2019-5804**	N/A	A-GOO-CHRO-060619/878
gpac					
gpac					
NULL	30-05-2019	4.3	An issue was discovered in	N/A	A-GPA-GPAC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			GPAC 0.7.1. There is a NULL pointer dereference in the function GetESD at isomedia/track.c in libgpac.a, as demonstrated by MP4Box. **CVE ID : CVE-2019-12481**		060619/879
NULL Pointer Dereference	30-05-2019	5	An issue was discovered in GPAC 0.7.1. There is a NULL pointer dereference in the function gf_isom_get_original_format_type at isomedia/drm_sample.c in libgpac.a, as demonstrated by MP4Box. **CVE ID : CVE-2019-12482**	N/A	A-GPA-GPAC-060619/880
Improper Restriction of Operations within the Bounds of a Memory Buffer	30-05-2019	6.8	An issue was discovered in GPAC 0.7.1. There is a heap-based buffer overflow in the function ReadGF_IPMPX_RemoveToolNotificationListener in odf/ipmpx_code.c in libgpac.a, as demonstrated by MP4Box. **CVE ID : CVE-2019-12483**	N/A	A-GPA-GPAC-060619/881
gpg-pgp_project					
gpg-pgp					
Improper Verification of Cryptographic Signature	16-05-2019	4.3	The signature verification routine in the Airmail GPG-PGP Plugin, versions 1.0 (9) and earlier, does not verify the status of the signature at all, which allows remote attackers to spoof arbitrary email signatures by crafting a signed email with an invalid signature. Also, it does not verify the validity of the signing key, which allows remote attackers	N/A	A-GPG-GPG--060619/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to spoof arbitrary email signatures by crafting a key with a fake user ID (email address) and injecting it into the user's keyring. **CVE ID : CVE-2019-8338**		
Haxx					
curl					
Integer Overflow or Wraparound	28-05-2019	4.3	An integer overflow in curl's URL API results in a buffer overflow in libcurl 7.62.0 to and including 7.64.1. **CVE ID : CVE-2019-5435**	https://curl.haxx.se/docs/CVE-2019-5435.html	A-HAX-CURL-060619/883
libcurl					
Improper Restriction of Operations within the Bounds of a Memory Buffer	28-05-2019	4.6	A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1. **CVE ID : CVE-2019-5436**	https://curl.haxx.se/docs/CVE-2019-5436.html	A-HAX-LIBC-060619/884
heidelberg					
prinect_archiver					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2019	4.3	A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in Heidelberg Prinect Archiver v2013 release 1.0. **CVE ID : CVE-2019-10685**	N/A	A-HEI-PRIN-060619/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Horde					
groupware					
Improper Control of Generation of Code ('Code Injection')	29-05-2019	6.5	Remote code execution was discovered in Horde Groupware Webmail 5.2.22 and 5.2.17. Horde/Form/Type.php contains a vulnerable class that handles image upload in forms. When the Horde_Form_Type_image method onSubmit() is called on uploads, it invokes the functions getImage() and _getUpload(), which uses unsanitized user input as a path to save the image. The unsanitized POST parameter object[photo][img][file] is saved in the $upload[img][file] PHP variable, allowing an attacker to manipulate the $tmp_file passed to move_uploaded_file() to save the uploaded file. By setting the parameter to (for example) ../usr/share/horde/static/bd.php, one can write a PHP backdoor inside the web root. The static/ destination folder is a good candidate to drop the backdoor because it is always writable in Horde installations. (The unsanitized POST parameter went probably unnoticed because it's never submitted by the forms, which default to securely using a random path.) **CVE ID : CVE-2019-9858**	N/A	A-HOR-GROU-060619/886
hybridgroup					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gobot					
Improper Certificate Validation	31-05-2019	5	An issue was discovered in Hybrid Group Gobot before 1.13.0. The mqtt subsystem skips verification of root CA certificates by default. **CVE ID : CVE-2019-12496**	N/A	A-HYB-GOBO-060619/887
IBM					
jazz_reporting_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-05-2019	3.5	IBM Jazz Reporting Service 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158974. **CVE ID : CVE-2019-4184**	https://www.ibm.com/support/docview.wss?uid=ibm10884604	A-IBM-JAZZ-060619/888
cognos_analytics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-05-2019	3.5	IBM Cognos Analytics 11.0, 11.1.0, and 11.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158335. **CVE ID : CVE-2019-4139**	N/A	A-IBM-COGN-060619/889
websphere_mq					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure Through Log Files	23-05-2019	2.1	IBM WebSphere MQ 8.0.0.0 through 8.0.0.9 and 9.0.0.0 through 9.1.1 could allow a local attacker to cause a denial of service within the error log reporting system. IBM X-Force ID: 156163. **CVE ID : CVE-2019-4039**	https://www.ibm.com/support/docview.wss?uid=ibm10870492	A-IBM-WEBS-060619/890
N/A	23-05-2019	7.2	IBM WebSphere MQ 8.0.0.0 through 8.0.0.9 and 9.0.0.0 through 9.1.1 could allow a local non privileged user to execute code as an administrator due to incorrect permissions set on MQ installation directories. IBM X-Force ID: 157190. **CVE ID : CVE-2019-4078**	https://www.ibm.com/support/docview.wss?uid=ibm10872876	A-IBM-WEBS-060619/891
api_connect					
Inadequate Encryption Strength	29-05-2019	5	IBM API Connect 5.0.0.0 through 5.0.8.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 159944. **CVE ID : CVE-2019-4256**	https://www.ibm.com/support/docview.wss?uid=ibm10882968	A-IBM-API_-060619/892
websphere_application_server					
Deserialization of Untrusted Data	17-05-2019	10	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 160445. **CVE ID : CVE-2019-4279**	https://www.ibm.com/support/docview.wss?uid=ibm10883628	A-IBM-WEBS-060619/893
bigfix_platform					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-05-2019	3.5	IBM BigFix Platform 9.2 and 9.5 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: 155885. **CVE ID : CVE-2019-4011**	https://www.ibm.com/support/docview.wss?uid=ibm10881996	A-IBM-BIGF-060619/894
N/A	20-05-2019	4	IBM BigFix Platform 9.2 and 9.5 could allow a low-privilege user to manipulate the UI into exposing interface elements and information normally restricted to administrators. IBM X-Force ID: 156570. **CVE ID : CVE-2019-4058**	https://www.ibm.com/support/docview.wss?uid=ibm10881996	A-IBM-BIGF-060619/895
qradar_security_information_and_event_manager					
Improper Certificate Validation	29-05-2019	4.3	IBM QRadar SIEM 7.2.8 WinCollect could allow an attacker to obtain sensitive information by spoofing a trusted entity using man in the middle techniques due to not validating or incorrectly validating a certificate. IBM X-Force ID: 160072. **CVE ID : CVE-2019-4264**	https://www.ibm.com/support/docview.wss?uid=ibm10885464	A-IBM-QRAD-060619/896
cloud_private					
Improper Input Validation	17-05-2019	5	IBM Cloud Private Kubernetes API server 2.1.0, 3.1.0, 3.1.1, and 3.1.2 can be used as an HTTP proxy to not only cluster internal but also external target IP addresses. IBM X-Force ID:	N/A	A-IBM-CLOU-060619/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			158145. **CVE ID : CVE-2019-4119**		
identityserver					
identityserver4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2019	4.3	IdentityServer IdentityServer4 through 2.4 has stored XSS via the httpContext to the host/Extensions/RequestLoggerMiddleware.cs LogForErrorContext method, which can be triggered by viewing a log. **CVE ID : CVE-2019-12250**	N/A	A-IDE-IDEN-060619/898
incsub					
hustle					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	29-05-2019	6.8	The Hustle (aka wordpress-popup) plugin 6.0.7 for WordPress is vulnerable to CSV Injection as it allows for injecting malicious code into a pop-up window. Successful exploitation grants an attacker with a right to execute malicious code on the administrator's computer through Excel functions as the plugin does not sanitize the user's input and allows insertion of any text. **CVE ID : CVE-2019-11872**	N/A	A-INC-HUST-060619/899
Intel					
acu_wizard					
N/A	17-05-2019	4.6	Improper directory permissions in Intel(R) ACU Wizard version 12.0.0.129 and earlier may allow an	N/A	A-INT-ACU_-060619/900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0138**		
scs_discovery_utility					
N/A	17-05-2019	4.6	Unquoted service path in the installer for the Intel(R) SCS Discovery Utility version 12.0.0.129 and earlier may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-11093**	N/A	A-INT-SCS_-060619/901
driver_&_support_assistant					
Improper Access Control	17-05-2019	2.1	Insufficient access control in Intel(R) Driver & Support Assistant version 19.3.12.3 and before may allow a privileged user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-11095**	N/A	A-INT-DRIV-060619/902
Improper Input Validation	17-05-2019	2.1	Insufficient input validation in Intel(R) Driver & Support Assistant version 19.3.12.3 and before may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-11114**	N/A	A-INT-DRIV-060619/903
converged_security_management_engine_firmware					
N/A	17-05-2019	4.6	Insufficient access control vulnerability in Dynamic Application Loader software for Intel(R) CSME before versions 11.8.65, 11.11.65, 11.22.65, 12.0.35 and Intel(R) TXE 3.1.65, 4.0.15 may allow an	N/A	A-INT-CONV-060619/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unprivileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0086**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.5	Buffer overflow in subsystem in Intel(R) CSME 12.0.0 through 12.0.34 may allow an unauthenticated user to potentially enable escalation of privilege via network access. **CVE ID : CVE-2019-0153**	N/A	A-INT-CONV-060619/905
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	4.6	Buffer overflow in subsystem in Intel(R) DAL before version 12.0.35 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0170**	N/A	A-INT-CONV-060619/906
active_management_technology					
Improper Input Validation	17-05-2019	4.6	Insufficient input validation vulnerability in subsystem for Intel(R) AMT before versions 11.8.65, 11.11.65, 11.22.65, 12.0.35 may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2019-0092**	N/A	A-INT-ACTI-060619/907
Improper Input Validation	17-05-2019	3.3	Insufficient input validation vulnerability in subsystem for Intel(R) AMT before versions 11.8.65, 11.11.65, 11.22.65, 12.0.35 may allow an	N/A	A-INT-ACTI-060619/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to potentially enable denial of service via adjacent network access. **CVE ID : CVE-2019-0094**		
Out-of-bounds Write	17-05-2019	5.2	Out of bound write vulnerability in subsystem for Intel(R) AMT before versions 11.8.65, 11.11.65, 11.22.65, 12.0.35 may allow an authenticated user to potentially enable escalation of privilege via adjacent network access. **CVE ID : CVE-2019-0096**	N/A	A-INT-ACTI-060619/909
graphics_driver					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	2.1	Insufficient bounds checking in Intel(R) Graphics Drivers before version 10.18.14.5067 (aka 15.36.x.5067) and 10.18.10.5069 (aka 15.33.x.5069) may allow an authenticated user to potentially enable a denial of service via local access. **CVE ID : CVE-2019-0113**	N/A	A-INT-GRAP-060619/910
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-05-2019	1.9	A race condition in Intel(R) Graphics Drivers before version 10.18.14.5067 (aka 15.36.x.5067) and 10.18.10.5069 (aka 15.33.x.5069) may allow an authenticated user to potentially enable a denial of service via local access. **CVE ID : CVE-2019-0114**	N/A	A-INT-GRAP-060619/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-05-2019	2.1	Insufficient input validation in KMD module for Intel(R) Graphics Driver before version 10.18.14.5067 (aka 15.36.x.5067) and 10.18.10.5069 (aka 15.33.x.5069) may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0115**	N/A	A-INT-GRAP-060619/912
Out-of-bounds Read	17-05-2019	2.1	An out of bound read in KMD module for Intel(R) Graphics Driver before version 10.18.14.5067 (aka 15.36.x.5067) and 10.18.10.5069 (aka 15.33.x.5069) may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0116**	N/A	A-INT-GRAP-060619/913
unite					
Improper Input Validation	17-05-2019	5	Data Corruption in Intel Unite(R) Client before version 3.3.176.13 may allow an unauthenticated user to potentially cause a denial of service via network access. **CVE ID : CVE-2019-0132**	N/A	A-INT-UNIT-060619/914
N/A	17-05-2019	7.5	A logic issue in Intel Unite(R) Client for Android prior to version 4.0 may allow a remote attacker to potentially enable escalation of privilege via network access. **CVE ID : CVE-2019-0172**	N/A	A-INT-UNIT-060619/915
Jenkins					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
warnings_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-05-2019	3.5	A cross-site scripting vulnerability in Jenkins Warnings NG Plugin 5.0.0 and earlier allowed attacker with Job/Configure permission to inject arbitrary JavaScript in build overview pages. **CVE ID : CVE-2019-10325**	N/A	A-JEN-WARN-060619/916
Cross-Site Request Forgery (CSRF)	31-05-2019	4.3	A cross-site request forgery vulnerability in Jenkins Warnings NG Plugin 5.0.0 and earlier allowed attackers to reset warning counts for future builds. **CVE ID : CVE-2019-10326**	N/A	A-JEN-WARN-060619/917
pluggable_authentication_module					
N/A	21-05-2019	4	A missing permission check in Jenkins PAM Authentication Plugin 1.5 and earlier, except 1.4.1 in PamSecurityRealm.DescriptorImpl#doTest allowed users with Overall/Read permission to obtain limited information about the file /etc/shadow and the user Jenkins is running as. **CVE ID : CVE-2019-10319**	N/A	A-JEN-PLUG-060619/918
credentials					
File and Directory Information Exposure	21-05-2019	4	Jenkins Credentials Plugin 2.1.18 and earlier allowed users with permission to create or update credentials to confirm the existence of files on the Jenkins master with an attacker-specified path, and	N/A	A-JEN-CRED-060619/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain the certificate content of files containing a PKCS#12 certificate. **CVE ID : CVE-2019-10320**		
pipeline_maven_integration					
Improper Restriction of XML External Entity Reference ('XXE')	31-05-2019	5.5	An XML external entities (XXE) vulnerability in Jenkins Pipeline Maven Integration Plugin 1.7.0 and earlier allowed attackers able to control a temporary directory's content on the agent running the Maven build to have Jenkins parse a maliciously crafted XML file that uses external entities for extraction of secrets from the Jenkins master, server-side request forgery, or denial-of-service attacks. **CVE ID : CVE-2019-10327**	N/A	A-JEN-PIPE-060619/920
pipeline_remote_loader					
Protection Mechanism Failure	31-05-2019	6.5	Jenkins Pipeline Remote Loader Plugin 1.4 and earlier provided a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection. **CVE ID : CVE-2019-10328**	N/A	A-JEN-PIPE-060619/921
Jfrog					
artifactory					
Cross-Site Request Forgery (CSRF)	31-05-2019	4.3	A cross-site request forgery vulnerability in Jenkins Artifactory Plugin 3.2.2 and earlier in ArtifactoryBuilder.DescriptorImpl#doTestConnection allowed users with	N/A	A-JFR-ARTI-060619/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10321**		
N/A	31-05-2019	4	A missing permission check in Jenkins Artifactory Plugin 3.2.2 and earlier in ArtifactoryBuilder.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-10322**	N/A	A-JFR-ARTI-060619/923
N/A	31-05-2019	4	A missing permission check in Jenkins Artifactory Plugin 3.2.2 and earlier in various 'fillCredentialsIdItems' methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2019-10323**	N/A	A-JFR-ARTI-060619/924
Cross-Site Request Forgery (CSRF)	31-05-2019	4.3	A cross-site request forgery vulnerability in Jenkins Artifactory Plugin 3.2.2 and earlier in ReleaseAction#doSubmit, GradleReleaseApiAction#doStaging, MavenReleaseApiAction#doSta	N/A	A-JFR-ARTI-060619/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ging, and UnifiedPromoteBuildAction#doSubmit allowed attackers to schedule a release build, perform release staging for Gradle and Maven projects, and promote previously staged builds, respectively. **CVE ID : CVE-2019-10324**		
Joomla					
Joomla!					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-05-2019	4.3	An issue was discovered in Joomla! before 3.9.6. The debug views of com_users do not properly escape user supplied data, which leads to a potential XSS attack vector. **CVE ID : CVE-2019-11809**	N/A	A-JOO-JOOM-060619/926
Jreast					
jr_east_japan					
Improper Access Control	17-05-2019	6.4	JR East Japan train operation information push notification App for Android version 1.2.4 and earlier allows remote attackers to bypass access restriction to obtain or alter the user's registered information via unspecified vectors. **CVE ID : CVE-2019-5954**	N/A	A-JRE-JR_E-060619/927
karamasoft					
ultimateeditor					
Unrestricted Upload of	24-05-2019	7.5	Karamasoft UltimateEditor 1 does not ensure that an uploaded file is an image or	N/A	A-KAR-ULTI-060619/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			document (neither file types nor extensions are restricted). The attacker must use the Attach icon to perform an upload. An uploaded file is accessible under the UltimateEditorInclude/UserFiles/ URI. **CVE ID : CVE-2019-12150**		
Kentico					
kentico					
Improper Input Validation	22-05-2019	6.4	Kentico 11 through 12 lets attackers upload and explore files without authentication via the cmsmodules/medialibrary/formcontrols/liveselectors/insertimageormedia/tabs_media.aspx URI. **CVE ID : CVE-2019-12102**	N/A	A-KEN-KENT-060619/929
Kibokolabs					
hostel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2019	4.3	XSS exists in the Kiboko Hostel plugin before 1.1.4 for WordPress. **CVE ID : CVE-2019-12345**	N/A	A-KIB-HOST-060619/930
leanify_project					
leanify					
Out-of-bounds	23-05-2019	4.3	Leanify 0.4.3 allows remote attackers to trigger an out-of-bounds write (1024 bytes) via a	N/A	A-LEA-LEAN-060619/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			modified input file. **CVE ID : CVE-2019-12298**		
Lemonldap-ng					
lemonldap					
Improper Access Control	22-05-2019	7.5	LemonLDAP::NG -2.0.3 has Incorrect Access Control. **CVE ID : CVE-2019-12046**	N/A	A-LEM-LEMO-060619/932
Libreswan					
libreswan					
NULL Pointer Dereference	24-05-2019	5	In Libreswan before 3.28, an assertion failure can lead to a pluto IKE daemon restart. An attacker can trigger a NULL pointer dereference by sending two IKEv2 packets (init_IKE and delete_IKE) in 3des_cbc mode to a Libreswan server. This affects send_v2N_spi_response_from_state in programs/pluto/ikev2_send.c when built with Network Security Services (NSS). **CVE ID : CVE-2019-12312**	N/A	A-LIB-LIBR-060619/933
libsdl					
sdl2_image					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a heap-based buffer overflow in the SDL2_image function IMG_LoadPCX_RW at IMG_pcx.c. **CVE ID : CVE-2019-12216**	N/A	A-LIB-SDL2-060619/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a NULL pointer dereference in the SDL stdio_read function in file/SDL_rwops.c. **CVE ID : CVE-2019-12217**	N/A	A-LIB-SDL2-060619/935
NULL Pointer Dereference	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a NULL pointer dereference in the SDL2_image function IMG_LoadPCX_RW at IMG_pcx.c. **CVE ID : CVE-2019-12218**	N/A	A-LIB-SDL2-060619/936
Double Free	20-05-2019	6.8	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is an invalid free error in the SDL function SDL_SetError_REAL at SDL_error.c. **CVE ID : CVE-2019-12219**	N/A	A-LIB-SDL2-060619/937
Out-of-bounds Read	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is an out-of-bounds read in the SDL function SDL_FreePalette_REAL at video/SDL_pixels.c.	N/A	A-LIB-SDL2-060619/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-12220		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a SEGV in the SDL function SDL_free_REAL at stdlib/SDL_malloc.c. **CVE ID : CVE-2019-12221**	N/A	A-LIB-SDL2-060619/939
simple_directmedia_layer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a heap-based buffer overflow in the SDL2_image function IMG_LoadPCX_RW at IMG_pcx.c. **CVE ID : CVE-2019-12216**	N/A	A-LIB-SIMP-060619/940
NULL Pointer Dereference	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a NULL pointer dereference in the SDL stdio_read function in file/SDL_rwops.c. **CVE ID : CVE-2019-12217**	N/A	A-LIB-SIMP-060619/941
NULL Pointer Dereference	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a NULL pointer dereference in the SDL2_image	N/A	A-LIB-SIMP-060619/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function IMG_LoadPCX_RW at IMG_pcx.c. **CVE ID : CVE-2019-12218**		
Double Free	20-05-2019	6.8	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is an invalid free error in the SDL function SDL_SetError_REAL at SDL_error.c. **CVE ID : CVE-2019-12219**	N/A	A-LIB-SIMP-060619/943
Out-of-bounds Read	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is an out-of-bounds read in the SDL function SDL_FreePalette_REAL at video/SDL_pixels.c. **CVE ID : CVE-2019-12220**	N/A	A-LIB-SIMP-060619/944
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a SEGV in the SDL function SDL_free_REAL at stdlib/SDL_malloc.c. **CVE ID : CVE-2019-12221**	N/A	A-LIB-SIMP-060619/945
Out-of-bounds Read	20-05-2019	4.3	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9. There is an out-of-bounds read in the function SDL_InvalidateMap at	N/A	A-LIB-SIMP-060619/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			video/SDL_pixels.c. **CVE ID : CVE-2019-12222**		
macdown_project					
macdown					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-05-2019	4.6	MacDown 0.7.1 allows directory traversal, for execution of arbitrary programs, via a file:/// or ../ substring in a shared note. **CVE ID : CVE-2019-12138**	N/A	A-MAC-MACD-060619/947
Improper Input Validation	17-05-2019	6.8	MacDown 0.7.1 (870) allows remote code execution via a file:\\\ URI, with a .app pathname, in the HREF attribute of an A element. This is different from CVE-2019-12138. **CVE ID : CVE-2019-12173**	N/A	A-MAC-MACD-060619/948
matomo					
matomo					
Information Exposure	20-05-2019	4	** DISPUTED ** A full path disclosure vulnerability was discovered in Matomo v3.9.1 where a user can trigger a particular error to discover the full path of Matomo on the disk, because lastError.file is used in plugins/CorePluginsAdmin/templates/safemode.twig. NOTE: the vendor disputes the significance of this issue, stating "avoid reporting path disclosures, as we don't	N/A	A-MAT-MATO-060619/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			consider them as security vulnerabilities." **CVE ID : CVE-2019-12215**		
Microsoft					
nuget					
Improper Access Control	16-05-2019	2.1	A tampering vulnerability exists in the NuGet Package Manager for Linux and Mac that could allow an authenticated attacker to modify contents of the intermediate build folder (by default "obj"), aka 'NuGet Package Manager Tampering Vulnerability'. **CVE ID : CVE-2019-0976**	N/A	A-MIC-NUGE-060619/950
visual_studio					
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0727**	N/A	A-MIC-VISU-060619/951
chakracore					
Improper Restriction of Operations within the	16-05-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption	N/A	A-MIC-CHAK-060619/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Vulnerability'. This CVE ID is unique from CVE-2019-0884, CVE-2019-0918. **CVE ID : CVE-2019-0911**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0912**	N/A	A-MIC-CHAK-060619/953
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0913**	N/A	A-MIC-CHAK-060619/954
Improper	16-05-2019	7.6	A remote code execution	N/A	A-MIC-CHAK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0914**		060619/955
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0915**	N/A	A-MIC-CHAK-060619/956
Improper Restriction of Operations within the Bounds	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption	N/A	A-MIC-CHAK-060619/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0916**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0917**	N/A	A-MIC-CHAK-060619/958
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0923, CVE-2019-	N/A	A-MIC-CHAK-060619/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0922**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0924**	N/A	A-MIC-CHAK-060619/960
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0925**	N/A	A-MIC-CHAK-060619/961
Improper	16-05-2019	7.6	A remote code execution	N/A	A-MIC-CHAK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0927**		060619/962
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0937. **CVE ID : CVE-2019-0933**	N/A	A-MIC-CHAK-060619/963
Improper Restriction of Operations within the Bounds	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption	N/A	A-MIC-CHAK-060619/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933. **CVE ID : CVE-2019-0937**		
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0911, CVE-2019-0918. **CVE ID : CVE-2019-0884**	N/A	A-MIC-EDGE-060619/965
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0884, CVE-2019-0918. **CVE ID : CVE-2019-0911**	N/A	A-MIC-EDGE-060619/966
Improper Restriction of Operations within the Bounds of a	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is	N/A	A-MIC-EDGE-060619/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			unique from CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0912**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0913**	N/A	A-MIC-EDGE-060619/968
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-	N/A	A-MIC-EDGE-060619/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0914**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0915**	N/A	A-MIC-EDGE-060619/970
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0916**	N/A	A-MIC-EDGE-060619/971
Improper Restrictio	16-05-2019	7.6	A remote code execution vulnerability exists in the way	N/A	A-MIC-EDGE-060619/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0917**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0922**	N/A	A-MIC-EDGE-060619/973
Improper Restriction of Operations within the Bounds of a	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is	N/A	A-MIC-EDGE-060619/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0923**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0924**	N/A	A-MIC-EDGE-060619/975
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-	N/A	A-MIC-EDGE-060619/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0927, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0925**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. **CVE ID : CVE-2019-0926**	N/A	A-MIC-EDGE-060619/977
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0933, CVE-2019-0937. **CVE ID : CVE-2019-0927**	N/A	A-MIC-EDGE-060619/978
Improper Restriction of Operations within the Bounds of a Memory	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-	N/A	A-MIC-EDGE-060619/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0937. **CVE ID : CVE-2019-0933**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0912, CVE-2019-0913, CVE-2019-0914, CVE-2019-0915, CVE-2019-0916, CVE-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0933. **CVE ID : CVE-2019-0937**	N/A	A-MIC-EDGE-060619/980
N/A	16-05-2019	6.8	An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser, aka 'Microsoft Edge Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0938**	N/A	A-MIC-EDGE-060619/981
Improper Restriction of Operations within the	16-05-2019	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'.	N/A	A-MIC-EDGE-060619/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			**CVE ID : CVE-2019-0940**		
office					
N/A	16-05-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0946, CVE-2019-0947. **CVE ID : CVE-2019-0945**	N/A	A-MIC-OFFI-060619/983
N/A	16-05-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0945, CVE-2019-0947. **CVE ID : CVE-2019-0946**	N/A	A-MIC-OFFI-060619/984
N/A	16-05-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0945, CVE-2019-	N/A	A-MIC-OFFI-060619/985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0946. **CVE ID : CVE-2019-0947**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0953**	N/A	A-MIC-OFFI-060619/986
office_365_proplus					
N/A	16-05-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0945, CVE-2019-0947. **CVE ID : CVE-2019-0946**	N/A	A-MIC-OFFI-060619/987
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0953**	N/A	A-MIC-OFFI-060619/988
internet_explorer					
Improper Restriction of	16-05-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles	N/A	A-MIC-INTE-060619/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0911, CVE-2019-0918. **CVE ID : CVE-2019-0884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0884, CVE-2019-0918. **CVE ID : CVE-2019-0911**	N/A	A-MIC-INTE-060619/990
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0884, CVE-2019-0911. **CVE ID : CVE-2019-0918**	N/A	A-MIC-INTE-060619/991
Improper Input Validation	16-05-2019	4.3	An spoofing vulnerability exists when Internet Explorer improperly handles URLs, aka 'Internet Explorer Spoofing Vulnerability'. **CVE ID : CVE-2019-0921**	N/A	A-MIC-INTE-060619/992
Improper Restriction of Operations within the	16-05-2019	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory	N/A	A-MIC-INTE-060619/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Corruption Vulnerability'. **CVE ID : CVE-2019-0929**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory, aka 'Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0930**	N/A	A-MIC-INTE-060619/994
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2019-0940**	N/A	A-MIC-INTE-060619/995
N/A	16-05-2019	6.8	A security feature bypass vulnerability exists when urlmon.dll improperly handles certain Mark of the Web queries, aka 'Internet Explorer Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0995**	N/A	A-MIC-INTE-060619/996
.net_core					
Improper Input Validation	16-05-2019	5	A denial of service vulnerability exists when .NET Framework and .NET Core improperly process RegEx strings, aka '.NET Framework and .NET Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0980, CVE-2019-0981.	N/A	A-MIC-.NET-060619/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0820		
N/A	16-05-2019	5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0820, CVE-2019-0981. **CVE ID : CVE-2019-0980**	N/A	A-MIC-.NET-060619/998
N/A	16-05-2019	5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0820, CVE-2019-0980. **CVE ID : CVE-2019-0981**	N/A	A-MIC-.NET-060619/999
.net_framework					
Improper Input Validation	16-05-2019	5	A denial of service vulnerability exists when .NET Framework and .NET Core improperly process RegEx strings, aka '.NET Framework and .NET Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0980, CVE-2019-0981. **CVE ID : CVE-2019-0820**	N/A	A-MIC-.NET-060619/1000
Improper Restriction of Operations within the Bounds	16-05-2019	2.1	A denial of service vulnerability exists when .NET Framework improperly handles objects in heap memory, aka '.NET Framework Denial of Service Vulnerability'.	N/A	A-MIC-.NET-060619/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			**CVE ID : CVE-2019-0864**		
N/A	16-05-2019	5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0820, CVE-2019-0981. **CVE ID : CVE-2019-0980**	N/A	A-MIC-.NET-060619/1002
N/A	16-05-2019	5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0820, CVE-2019-0980. **CVE ID : CVE-2019-0981**	N/A	A-MIC-.NET-060619/1003
visual_studio_2017					
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0727**	N/A	A-MIC-VISU-060619/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
asp.net_core					
N/A	16-05-2019	5	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2019-0982**	N/A	A-MIC-ASP.-060619/1005
sharepoint_server					
Improper Input Validation	16-05-2019	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0950, CVE-2019-0951. **CVE ID : CVE-2019-0949**	N/A	A-MIC-SHAR-060619/1006
Improper Input Validation	16-05-2019	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0949, CVE-2019-0951. **CVE ID : CVE-2019-0950**	N/A	A-MIC-SHAR-060619/1007
N/A	16-05-2019	6.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is	N/A	A-MIC-SHAR-060619/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-0958. **CVE ID : CVE-2019-0957**		
N/A	16-05-2019	6.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0957. **CVE ID : CVE-2019-0958**	N/A	A-MIC-SHAR-060619/1009
word					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0953**	N/A	A-MIC-WORD-060619/1010
sharepoint_enterprise_server					
N/A	16-05-2019	6	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0952**	N/A	A-MIC-SHAR-060619/1011
Information Exposure	16-05-2019	4	An information disclosure vulnerability exists when Microsoft SharePoint Server does not properly sanitize a	N/A	A-MIC-SHAR-060619/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Server Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0956**		
N/A	16-05-2019	6.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0958. **CVE ID : CVE-2019-0957**	N/A	A-MIC-SHAR-060619/1013
office_online_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0953**	N/A	A-MIC-OFFI-060619/1014
sharepoint_foundation					
Improper Input Validation	16-05-2019	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0950, CVE-2019-0951.	N/A	A-MIC-SHAR-060619/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0949		
Improper Input Validation	16-05-2019	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0949, CVE-2019-0951. **CVE ID : CVE-2019-0950**	N/A	A-MIC-SHAR-060619/1016
Improper Input Validation	16-05-2019	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0949, CVE-2019-0950. **CVE ID : CVE-2019-0951**	N/A	A-MIC-SHAR-060619/1017
N/A	16-05-2019	6	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0952**	N/A	A-MIC-SHAR-060619/1018
Information Exposure	16-05-2019	4	An information disclosure vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint	N/A	A-MIC-SHAR-060619/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0956**		
N/A	16-05-2019	6.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0957. **CVE ID : CVE-2019-0958**	N/A	A-MIC-SHAR-060619/1020
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-05-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. **CVE ID : CVE-2019-0963**	N/A	A-MIC-SHAR-060619/1021
skype					
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists in Skype for Android, aka 'Skype for Android Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0932**	N/A	A-MIC-SKYP-060619/1022
team_foundation_server					
Improper Neutralization of Input During	16-05-2019	3.5	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided	N/A	A-MIC-TEAM-060619/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0979. **CVE ID : CVE-2019-0872**		
Information Exposure	16-05-2019	9	An information disclosure vulnerability exists when Azure DevOps Server and Microsoft Team Foundation Server do not properly sanitize a specially crafted authentication request to an affected server, aka 'Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0971**	N/A	A-MIC-TEAM-060619/1024
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-05-2019	3.5	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0872. **CVE ID : CVE-2019-0979**	N/A	A-MIC-TEAM-060619/1025
visual_studio_2019					
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the	N/A	A-MIC-VISU-060619/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system, aka 'Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0727**		
sql_server					
Information Exposure	16-05-2019	4	An information disclosure vulnerability exists in Microsoft SQL Server Analysis Services when it improperly enforces metadata permissions, aka 'Microsoft SQL Server Analysis Services Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0819**	N/A	A-MIC-SQL_-060619/1027
office_365					
N/A	16-05-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0946, CVE-2019-0947. **CVE ID : CVE-2019-0945**	N/A	A-MIC-OFFI-060619/1028
azure_active_directory_connect					
N/A	16-05-2019	3.5	An elevation of privilege vulnerability exists in Microsoft Azure Active Directory Connect build 1.3.20.0, which allows an attacker to execute two PowerShell cmdlets in context of a privileged account, and perform privileged actions.To	N/A	A-MIC-AZUR-060619/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this, an attacker would need to authenticate to the AzureÂ? AD Connect server, aka 'Microsoft Azure AD Connect Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1000**		
dynamics_365					
N/A	16-05-2019	4.3	A security feature bypass vulnerability exists in Dynamics On Premise, aka 'Microsoft Dynamics On-Premise Security Feature Bypass'. **CVE ID : CVE-2019-1008**	N/A	A-MIC-DYNA-060619/1030
dynamics_crm_2015					
N/A	16-05-2019	4.3	A security feature bypass vulnerability exists in Dynamics On Premise, aka 'Microsoft Dynamics On-Premise Security Feature Bypass'. **CVE ID : CVE-2019-1008**	N/A	A-MIC-DYNA-060619/1031
Mylittleforum					
my_little_forum					
Cross-Site Request Forgery (CSRF)	21-05-2019	5.8	my little forum before 2.4.20 allows CSRF to delete posts, as demonstrated by mode=posting&delete_posting. **CVE ID : CVE-2019-12253**	N/A	A-MYL-MY_L-060619/1032
Nagios					
nagios_xi					
Improper Neutralization of Special Elements	22-05-2019	7.5	Nagios XI 5.6.1 allows SQL injection via the username parameter to login.php?forgotpass (aka the	N/A	A-NAG-NAGI-060619/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			reset password form). **CVE ID : CVE-2019-12279**		
Netgate					
Pfsense					
Improper Access Control	20-05-2019	6.5	Incorrect access control in the WebUI in OPNsense before version 19.1.8, and pfsense before 2.4.4-p3 allows remote authenticated users to escalate privileges to administrator via a specially crafted request. **CVE ID : CVE-2019-11816**	https://www.netgate.com/blog/pfsense-2-4-4-release-p3-now-available.html	A-NET-PFSE-060619/1034
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-05-2019	4.3	In pfSense 2.4.4-p3, a stored XSS vulnerability occurs when attackers inject a payload into the Name or Description field via an acme_accountkeys_edit.php action. The vulnerability occurs due to input validation errors. **CVE ID : CVE-2019-12347**	N/A	A-NET-PFSE-060619/1035
Nginx					
njs					
Improper Restriction of Operations within the Bounds of a Memory	20-05-2019	7.5	njs through 0.3.1, used in NGINX, has a heap-based buffer overflow in nxt_utf8_encode in nxt_utf8.c. **CVE ID : CVE-2019-12206**	N/A	A-NGI-NJS-060619/1036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-05-2019	7.5	njs through 0.3.1, used in NGINX, has a heap-based buffer over-read in nxt_utf8_decode in nxt/nxt_utf8.c. **CVE ID : CVE-2019-12207**	N/A	A-NGI-NJS-060619/1037
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-05-2019	7.5	njs through 0.3.1, used in NGINX, has a heap-based buffer overflow in njs_function_native_call in njs/njs_function.c. **CVE ID : CVE-2019-12208**	N/A	A-NGI-NJS-060619/1038
openwrt					
luci					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-05-2019	7.5	In OpenWrt LuCI through 0.10, the endpoints admin/status/realtime/bandwidth_status and admin/status/realtime/wireless_status of the web application are affected by a command injection vulnerability. **CVE ID : CVE-2019-12272**	N/A	A-OPE-LUCI-060619/1039
Oracle					
enterprise_manager_ops_center					
Improper Access	24-05-2019	6.3	Vulnerability in the Enterprise Manager Ops Center	N/A	A-ORA-ENTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			component of Oracle Enterprise Manager Products Suite (subcomponent: Services Integration). The supported version that is affected is 12.3.3. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Ops Center. While the vulnerability is in Enterprise Manager Ops Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Enterprise Manager Ops Center. CVSS 3.0 Base Score 6.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2019-2726**		060619/1040
Otrs					
otrs					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2019	3.5	An issue was discovered in Open Ticket Request System (OTRS) 7.x through 7.0.6, Community Edition 6.0.x through 6.0.17, and OTRSAppointmentCalendar 5.0.x through 5.0.12. An attacker who is logged into OTRS as an agent with appropriate permissions may create a carefully crafted calendar appointment in order	https://community.otrs.com/security-advisory-2019-06-security-update-for-otrs-framework/	A-OTR-OTRS-060619/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to cause execution of JavaScript in the context of OTRS. **CVE ID : CVE-2019-10066**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2019	3.5	An issue was discovered in Open Ticket Request System (OTRS) 7.x through 7.0.6 and Community Edition 5.0.x through 5.0.35 and 6.0.x through 6.0.17. An attacker who is logged into OTRS as an agent user with appropriate permissions may manipulate the URL to cause execution of JavaScript in the context of OTRS. **CVE ID : CVE-2019-10067**	https://community.otrs.com/security-advisory-2019-05-security-update-for-otrs-framework/	A-OTR-OTRS-060619/1042
XML Injection (aka Blind XPath Injection)	21-05-2019	4	An issue was discovered in Open Ticket Request System (OTRS) 5.x through 5.0.34, 6.x through 6.0.17, and 7.x through 7.0.6. An attacker who is logged into OTRS as an agent user with appropriate permissions may try to import carefully crafted Report Statistics XML that will result in reading of arbitrary files on the OTRS filesystem. **CVE ID : CVE-2019-9892**	N/A	A-OTR-OTRS-060619/1043
Ovirt					
cockpit-ovirt					
N/A	17-05-2019	2.1	During HE deployment via cockpit-ovirt, cockpit-ovirt generates an ansible variable file `/var/lib/ovirt-hosted-engine-setup/cockpit/ansibleVarFileXXXXXX.var` which contains the admin and the appliance passwords as plain-text. At the	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10139	A-OVI-COCK-060619/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the deployment procedure, these files are deleted. **CVE ID : CVE-2019-10139**		
Pandasecurity					
panda_gold_protection					
N/A	23-05-2019	10	Insecure permissions of the section object Global\PandaDevicesAgentSharedMemory and the event Global\PandaDevicesAgentSharedMemoryChange in Panda products before 18.07.03 allow attackers to queue an event (as an encrypted JSON string) to the system service AgentSvc.exe, which leads to privilege escalation when the CmdLineExecute event is queued. This affects Panda Antivirus, Panda Antivirus Pro, Panda Dome, Panda Global Protection, Panda Gold Protection, and Panda Internet Security. **CVE ID : CVE-2019-12042**	https://www.pandasecurity.com/usa/support/card?id=100063	A-PAN-PAND-060619/1045
Percona					
percona_server					
Improper Authentication	23-05-2019	10	The Percona Server 5.6.44-85.0-1 packages for Debian and Ubuntu suffered an issue where the server would reset the root password to a blank value upon an upgrade. This was fixed in 5.6.44-85.0-2. **CVE ID : CVE-2019-12301**	N/A	A-PER-PERC-060619/1046
Pfsense					
pfsense					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	20-05-2019	6.5	Incorrect access control in the WebUI in OPNsense before version 19.1.8, and pfsense before 2.4.4-p3 allows remote authenticated users to escalate privileges to administrator via a specially crafted request. **CVE ID : CVE-2019-11816**	https://www.netgate.com/blog/pfsense-2-4-4-release-p3-now-available.html	A-PFS-PFSE-060619/1047
Phome					
empirecms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2019	4.3	EmpireCMS 7.5.0 has XSS via the from parameter to e/member/doaction.php, as demonstrated by a CSRF payload that changes the dynamic page template. The attacker can choose to resend the e/template/member/regsend.php registered activation mail page. **CVE ID : CVE-2019-12361**	N/A	A-PHO-EMPI-060619/1048
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2019	4.3	EmpireCMS 7.5.0 has XSS via the HTTP Referer header to e/member/doaction.php. **CVE ID : CVE-2019-12362**	N/A	A-PHO-EMPI-060619/1049
phprelativepath_project					
phprelativepath					
Improper Neutralization of	31-05-2019	4.3	An XSS vulnerability exists in PHPRelativePath (aka Relative Path) through 1.0.2 via the	N/A	A-PHP-PHPR-060619/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			RelativePath.Example1.php path parameter. **CVE ID : CVE-2019-12507**		
Prestashop					
prestashop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2019	4.3	In PrestaShop 1.7.5.2, the shop_country parameter in the install/index.php installation script/component is affected by Reflected XSS. Exploitation by a malicious actor requires the user to follow the initial stages of the setup (accepting terms and conditions) before executing the malicious link. **CVE ID : CVE-2019-11876**	N/A	A-PRE-PRES-060619/1051
Qemu					
qemu					
NULL Pointer Dereference	24-05-2019	5	interface_release_resource in hw/display/qxl.c in QEMU 4.0.0 has a NULL pointer dereference. **CVE ID : CVE-2019-12155**	N/A	A-QEM-QEMU-060619/1052
Integer Overflow or Wraparound	22-05-2019	5	** DISPUTED ** QEMU 3.0.0 has an Integer Overflow because the qga/commands*.c files do not check the length of the argument list or the number of environment variables. NOTE: This has been disputed as not exploitable. **CVE ID : CVE-2019-12247**	N/A	A-QEM-QEMU-060619/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redhat					
libvirt					
N/A	22-05-2019	6.5	A vulnerability was found in libvirt >= 4.1.0 in the virtlockd-admin.socket and virtlogd-admin.socket systemd units. A missing SocketMode configuration parameter allows any user on the host to connect using virtlockd-admin-sock or virtlogd-admin-sock and perform administrative tasks against the virtlockd and virtlogd daemons. **CVE ID : CVE-2019-10132**	N/A	A-RED-LIBV-060619/1054
Revive-adserver					
revive_adserver					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	28-05-2019	6.8	Use of cryptographically weak PRNG in the password recovery token generation of Revive Adserver < v4.2.1 causes a potential authentication bypass attack if an attacker exploits the password recovery functionality. In lib/OA/Dal/PasswordRecovery.php, the function generateRecoveryId() generates a password reset token that relies on the PHP uniqid function and consequently depends only on the current server time, which is often visible in an HTTP Date header. **CVE ID : CVE-2019-5440**	N/A	A-REV-REVI-060619/1055
Sensiolabs					
symfony					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-05-2019	3.5	In Symfony before 2.7.51, 2.8.x before 2.8.50, 3.x before 3.4.26, 4.x before 4.1.12, and 4.2.x before 4.2.7, validation messages are not escaped, which can lead to XSS when user input is included. This is related to symfony/framework-bundle. **CVE ID : CVE-2019-10909**	N/A	A-SEN-SYMF-060619/1056
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-05-2019	7.5	In Symfony before 2.7.51, 2.8.x before 2.8.50, 3.x before 3.4.26, 4.x before 4.1.12, and 4.2.x before 4.2.7, when service ids allow user input, this could allow for SQL Injection and remote code execution. This is related to symfony/dependency-injection. **CVE ID : CVE-2019-10910**	https://symfony.com/blog/cve-2019-10910-check-service-ids-are-valid	A-SEN-SYMF-060619/1057
Improper Authentication	16-05-2019	6	In Symfony before 2.7.51, 2.8.x before 2.8.50, 3.x before 3.4.26, 4.x before 4.1.12, and 4.2.x before 4.2.7, a vulnerability would allow an attacker to authenticate as a privileged user on sites with user registration and remember me login functionality enabled. This is related to symfony/security. **CVE ID : CVE-2019-10911**	https://symfony.com/blog/cve-2019-10911-add-a-separator-in-the-remember-me-cookie-hash	A-SEN-SYMF-060619/1058
Deserialization of Untrusted Data	16-05-2019	6.5	In Symfony before 2.8.50, 3.x before 3.4.26, 4.x before 4.1.12, and 4.2.x before 4.2.7, it is possible to cache objects that may contain bad user input. On serialization or unserialization,	https://symfony.com/blog/cve-2019-10912-prevent-	A-SEN-SYMF-060619/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this could result in the deletion of files that the current user has access to. This is related to symfony/cache and symfony/phpunit-bridge. **CVE ID : CVE-2019-10912**	destructors-with-side-effects-from-being-unserialized	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-05-2019	7.5	In Symfony before 2.7.51, 2.8.x before 2.8.50, 3.x before 3.4.26, 4.x before 4.1.12, and 4.2.x before 4.2.7, HTTP Methods provided as verbs or using the override header may be treated as trusted input, but they are not validated, possibly causing SQL injection or XSS. This is related to symfony/http-foundation. **CVE ID : CVE-2019-10913**	https://symfony.com/blog/cve-2019-10913-reject-invalid-http-method-overrides	A-SEN-SYMF-060619/1060
simplybook					
simplybook					
Unrestricted Upload of File with Dangerous Type	17-05-2019	7.5	SimplyBook.me through 2019-05-11 does not properly restrict File Upload which could allow remote code execution. **CVE ID : CVE-2019-11887**	https://news.simplybook.me/notification/	A-SIM-SIMP-060619/1061
Soumu					
electronic_reception_and_examination_of_application_for_radio_licenses					
Untrusted Search Path	17-05-2019	6.8	Untrusted search path vulnerability in Installer of Electronic reception and examination of application for radio licenses Online 1.0.9.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2019-5957**	N/A	A-SOU-ELEC-060619/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	17-05-2019	6.8	Untrusted search path vulnerability in Electronic reception and examination of application for radio licenses Offline 1.0.9.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2019-5958**	N/A	A-SOU-ELEC-060619/1063
Sqlite					
sqlite					
Out-of-bounds Read	30-05-2019	7.5	SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables. **CVE ID : CVE-2019-8457**	N/A	A-SQL-SQLI-060619/1064
synacor					
zimbra_collaboration_suite					
Deserialization of Untrusted Data	29-05-2019	7.5	Synacor Zimbra Collaboration Suite 8.7.x through 8.8.11 allows insecure object deserialization in the IMAP component. **CVE ID : CVE-2019-6980**	N/A	A-SYN-ZIMB-060619/1065
Server-Side Request Forgery (SSRF)	29-05-2019	4	Zimbra Collaboration Suite 8.7.x through 8.8.11 allows Blind SSRF in the Feed component. **CVE ID : CVE-2019-6981**	N/A	A-SYN-ZIMB-060619/1066
Improper Restriction of XML External Entity Reference ('XXE')	29-05-2019	7.5	mailboxd component in Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10 has an XML External Entity injection (XXE) vulnerability. **CVE ID : CVE-2019-9670**	N/A	A-SYN-ZIMB-060619/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tinycc					
tinycc					
Out-of-bounds Write	31-05-2019	4.3	An issue was discovered in Tiny C Compiler (aka TinyCC or TCC) 0.9.27. Compiling a crafted source file leads to a one-byte out-of-bounds write in the gsym_addr function in x86_64-gen.c. This occurs because tccasm.c mishandles section switches. **CVE ID : CVE-2019-12495**	N/A	A-TIN-TINY-060619/1068
Torproject					
tor_browser					
Information Exposure	27-05-2019	4.3	Tor Browser before 8.0.1 has an information exposure vulnerability. It allows remote attackers to detect the browser's UI locale by measuring a button width, even if the user has a "Don't send my language" setting. **CVE ID : CVE-2019-12383**	N/A	A-TOR-TOR_-060619/1069
typora					
typora					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-05-2019	6.8	Typora 0.9.9.24.6 on macOS allows directory traversal, for execution of arbitrary programs, via a file:/// or ../ substring in a shared note. **CVE ID : CVE-2019-12137**	N/A	A-TYP-TYPO-060619/1070
Improper Input	17-05-2019	6.8	Typora 0.9.9.21.1 (1913) allows arbitrary code execution	N/A	A-TYP-TYPO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			via a modified file: URL syntax in the HREF attribute of an AREA element, as demonstrated by file:\\\ on macOS or Linux, or file://C| on Windows. This is different from CVE-2019-12137. **CVE ID : CVE-2019-12172**		060619/1071
ucms_project					
ucms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-05-2019	6.5	sadmin/ceditpost.php in UCMS 1.4.7 allows SQL Injection via the index.php?do=sadmin_ceditpost cvalue parameter. **CVE ID : CVE-2019-12251**	N/A	A-UCM-UCMS-060619/1072
virim_project					
virim					
Deserialization of Untrusted Data	20-05-2019	7.5	The Virim plugin 0.4 for WordPress allows Insecure Deserialization via s_values, t_values, or c_values in graph.php. **CVE ID : CVE-2019-12240**	N/A	A-VIR-VIRI-060619/1073
Vtiger					
vtiger_crm					
Improper Neutralization of Special Elements used in an SQL	17-05-2019	6.5	SQL injection vulnerability in Vtiger CRM before 7.1.0 hotfix3 allows authenticated users to execute arbitrary SQL commands. **CVE ID : CVE-2019-11057**	N/A	A-VTI-VTIG-060619/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')					
webpagetest					
webpagetest					
Server-Side Request Forgery (SSRF)	17-05-2019	4	WPO WebPageTest 19.04 allows SSRF because ValidateURL in www/runtest.php does not consider octal encoding of IP addresses (such as 0300.0250 as a replacement for 192.168). **CVE ID : CVE-2019-12161**	N/A	A-WEB-WEBP-060619/1075
webport					
web_port					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-05-2019	4.3	Web Port 1.19.1 allows XSS via the /access/setup type parameter. **CVE ID : CVE-2019-12460**	N/A	A-WEB-WEB_-060619/1076
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-05-2019	4.3	Web Port 1.19.1 allows XSS via the /log type parameter. **CVE ID : CVE-2019-12461**	N/A	A-WEB-WEB_-060619/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wireshark					
wireshark					
Improper Control of Generation of Code ('Code Injection')	23-05-2019	5	In Wireshark 3.0.0 to 3.0.1, 2.6.0 to 2.6.8, and 2.4.0 to 2.4.14, the dissection engine could crash. This was addressed in epan/packet.c by restricting the number of layers and consequently limiting recursion. **CVE ID : CVE-2019-12295**	N/A	A-WIR-WIRE-060619/1078
Wolfssl					
wolfssl					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-05-2019	7.5	wolfSSL 4.0.0 has a Buffer Overflow in DoPreSharedKeys in tls13.c when a current identity size is greater than a client identity size. An attacker sends a crafted hello client packet over the network to a TLSv1.3 wolfSSL server. The length fields of the packet: record length, client hello length, total extensions length, PSK extension length, total identity length, and identity length contain their maximum value which is 2^16. The identity data field of the PSK extension of the packet contains the attack data, to be stored in the undefined memory (RAM) of the server. The size of the data is about 65 kB. Possibly the attacker can perform a remote code execution attack. **CVE ID : CVE-2019-11873**	N/A	A-WOL-WOLF-060619/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wpbookingsystem					
wp_booking_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-05-2019	6.5	The WP Booking System plugin 1.5.1 for WordPress has no CSRF protection, which allows attackers to reach certain SQL injection issues that require administrative access. **CVE ID : CVE-2019-12239**	N/A	A-WPB-WP_B-060619/1080
Wso2					
api_manager					
Unrestricted Upload of File with Dangerous Type	21-05-2019	5.5	An issue was discovered in WSO2 API Manager 2.6.0. It is possible for a logged-in user to upload, as API documentation, any type of file by changing the extension to an allowed one. **CVE ID : CVE-2019-6513**	N/A	A-WSO-API_-060619/1081
Zohocorp					
manageengine_servicedesk_plus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2019	4.3	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the SearchN.do search field. **CVE ID : CVE-2019-12189**	N/A	A-ZOH-MANA-060619/1082
N/A	21-05-2019	4	In Zoho ManageEngine ServiceDesk Plus through 10.5, users with the lowest privileges	N/A	A-ZOH-MANA-060619/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(guest) can view an arbitrary post by appending its number to the SDNotify.do?notifyModule=Solution&mode=E-Mail&notifyTo=SOLFORWARD&id= substring. **CVE ID : CVE-2019-12252**		
manageengine_adselfservice_plus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2019	4.3	In Zoho ManageEngine ADSelfService Plus 5.x through 5704, an authorization.do cross-site Scripting (XSS) vulnerability allows for an unauthenticated manipulation of the JavaScript code by injecting the HTTP form parameter adscsrf. An attacker can use this to capture a user's AD self-service password reset and MFA token. **CVE ID : CVE-2019-8346**	N/A	A-ZOH-MANA-060619/1084
manageengine_netflow_analyzer					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-05-2019	4	An issue was discovered in Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2. An Absolute Path Traversal vulnerability in the Administration zone, in /netflow/servlet/CReportPDFServlet (via the parameter schFilePath), allows remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory via any file name, such as a schFilePath=C:\boot.ini value. **CVE ID : CVE-2019-8925**	N/A	A-ZOH-MANA-060619/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	4.3	An issue was discovered in Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2. XSS exists in the Administration zone /netflow/jspui/popup1.jsp file via these GET parameters: bussAlert, customDev, and selSource. **CVE ID : CVE-2019-8926**	N/A	A-ZOH-MANA-060619/1086
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	4.3	An issue was discovered in Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2. XSS exists in the Administration zone /netflow/jspui/scheduleConfig.jsp file via these GET parameters: devSrc, emailId, excWeekModify, filterFlag, getFilter, mailReport, mset, popup, rep_schedule, rep_Type, schDesc, schName, schSource, selectDeviceDone, task, val10, and val11. **CVE ID : CVE-2019-8927**	N/A	A-ZOH-MANA-060619/1087
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-05-2019	4.3	An issue was discovered in Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2. XSS exists in /netflow/jspui/userManagementForm.jsp via these GET parameters: authMeth, passWord, pwd1, and userName. **CVE ID : CVE-2019-8928**	N/A	A-ZOH-MANA-060619/1088
Improper Neutralization of	17-05-2019	4.3	An issue was discovered in Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2.	N/A	A-ZOH-MANA-060619/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			XSS exists in the Administration zone /netflow/jspui/selectDevice.jsp file in these GET parameters: param and rtype. **CVE ID : CVE-2019-8929**		
Operating System					
bosch					
access_easy_controller_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-05-2019	7.5	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Video Recording Manager (VRM), Video Streaming Gateway (VSG), Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The vulnerability potentially allows the unauthorized execution of code in the system via the network interface. **CVE ID : CVE-2019-6957**	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-0403bt-cve-2019-6957_security_advisory_software_buffer_overflow.pdf	O-BOS-ACCE-060619/1090
Improper Access Control	29-05-2019	6.4	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Configuration Manager, Building Integration System (BIS) with Video Engine, Access	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-	O-BOS-ACCE-060619/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The RCP+ network port allows access without authentication. Adding authentication feature to the respective library fixes the issue. The issue is classified as "CWE-284: Improper Access Control." This vulnerability, for example, allows a potential attacker to delete video or read video data. **CVE ID : CVE-2019-6958**	0404bt-cve-2019-6958_security_advisory_improper_access_control.pdf	
dip_3000_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-05-2019	7.5	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Video Recording Manager (VRM), Video Streaming Gateway (VSG), Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The vulnerability potentially allows the unauthorized execution of code in the system via the network interface. **CVE ID : CVE-2019-6957**	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-0403bt-cve-2019-6957_security_advisory_software_buffer_overflow.pdf	O-BOS-DIP_-060619/1092
Improper Access Control	29-05-2019	6.4	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below,	https://media.boschsecurity.com/fs/media/p	O-BOS-DIP_-060619/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DIVAR IP 2000, 3000, 5000 and 7000, Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The RCP+ network port allows access without authentication. Adding authentication feature to the respective library fixes the issue. The issue is classified as "CWE-284: Improper Access Control." This vulnerability, for example, allows a potential attacker to delete video or read video data. **CVE ID : CVE-2019-6958**	b/security_advisories/bosch-2019-0404bt-cve-2019-6958_security_advisory_improper_access_control.pdf	
dip_7000_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-05-2019	7.5	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Video Recording Manager (VRM), Video Streaming Gateway (VSG), Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The vulnerability potentially allows the unauthorized execution of code in the system via the network interface. **CVE ID : CVE-2019-6957**	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-0403bt-cve-2019-6957_security_advisory_software_buffer_overflow.pdf	O-BOS-DIP_-060619/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	29-05-2019	6.4	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The RCP+ network port allows access without authentication. Adding authentication feature to the respective library fixes the issue. The issue is classified as "CWE-284: Improper Access Control." This vulnerability, for example, allows a potential attacker to delete video or read video data. **CVE ID : CVE-2019-6958**	https://media.boschsecurity.com/fs/media/pb/security_advisories/bosch-2019-0404bt-cve-2019-6958_security_advisory_improper_access_control.pdf	O-BOS-DIP_-060619/1095
Cisco					
nx-os					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-05-2019	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker with administrator credentials to execute arbitrary commands on the underlying operating system of an affected device with elevated privileges. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as	N/A	O-CIS-NX-O-060619/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. NX-OS versions prior to 8.3(1) are affected. NX-OS versions prior to 8.3(1) are affected. **CVE ID : CVE-2019-1780**		
Citrix					
netscaler_application_delivery_controller_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	5	A Buffer Overflow exists in Citrix NetScaler Gateway 10.5.x before 10.5.70.x, 11.1.x before 11.1.59.10, 12.0.x before 12.0.59.8, and 12.1.x before 12.1.49.23 and Citrix Application Delivery Controller 10.5.x before 10.5.70.x, 11.1.x before 11.1.59.10, 12.0.x before 12.0.59.8, and 12.1.x before 12.1.49.23. **CVE ID : CVE-2019-12044**	N/A	O-CIT-NETS-060619/1097
netscaler_gateway_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-05-2019	5	A Buffer Overflow exists in Citrix NetScaler Gateway 10.5.x before 10.5.70.x, 11.1.x before 11.1.59.10, 12.0.x before 12.0.59.8, and 12.1.x before 12.1.49.23 and Citrix Application Delivery Controller 10.5.x before 10.5.70.x, 11.1.x before 11.1.59.10, 12.0.x before 12.0.59.8, and 12.1.x before	N/A	O-CIT-NETS-060619/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.1.49.23. **CVE ID : CVE-2019-12044**		
Debian					
debian_linux					
N/A	23-05-2019	4.3	An issue is present in Apache ZooKeeper 1.0.0 to 3.4.13 and 3.5.0-alpha to 3.5.4-beta. ZooKeeper?s getACL() command doesn?t check any permission when retrieves the ACLs of the requested node and returns all information contained in the ACL Id field as plaintext string. DigestAuthenticationProvider overloads the Id field with the hash value that is used for user authentication. As a consequence, if Digest Authentication is in use, the unsalted hash value will be disclosed by getACL() request for unauthenticated or unprivileged users. **CVE ID : CVE-2019-0201**	https://zookeeper.apache.org/security.html#CVE-2019-0201	O-DEB-DEBI-060619/1099
Improper Access Control	22-05-2019	7.5	LemonLDAP::NG -2.0.3 has Incorrect Access Control. **CVE ID : CVE-2019-12046**	N/A	O-DEB-DEBI-060619/1100
Information Exposure	17-05-2019	5	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint, the service has the mysql-connector-java jar (8.0.14 or earlier) in the classpath, and an attacker can	N/A	O-DEB-DEBI-060619/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			host a crafted MySQL server reachable by the victim, an attacker can send a crafted JSON message that allows them to read arbitrary local files on the server. This occurs because of missing com.mysql.cj.jdbc.admin.MiniAdmin validation. **CVE ID : CVE-2019-12086**		
N/A	16-05-2019	6.8	It was found that in ghostscript some privileged operators remained accessible from various places after the CVE-2019-6116 fix. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constrains imposed by -dSAFER. Ghostscript versions before 9.27 are vulnerable. **CVE ID : CVE-2019-3839**	N/A	O-DEB-DEBI-060619/1102
Out-of-bounds Read	23-05-2019	4.3	Lack of correct bounds checking in Skia in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. **CVE ID : CVE-2019-5798**	N/A	O-DEB-DEBI-060619/1103
XML Injection (aka Blind XPath Injection)	21-05-2019	4	An issue was discovered in Open Ticket Request System (OTRS) 5.x through 5.0.34, 6.x through 6.0.17, and 7.x through 7.0.6. An attacker who is logged into OTRS as an agent user with appropriate permissions may try to import carefully crafted	N/A	O-DEB-DEBI-060619/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Report Statistics XML that will result in reading of arbitrary files on the OTRS filesystem. **CVE ID : CVE-2019-9892**		
Emerson					
liebert_challenger_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-05-2019	4.3	httpGetSet/httpGet.htm on Emerson Network Power Liebert Challenger 5.1E0.5 devices allows XSS via the statusstr parameter. **CVE ID : CVE-2019-12167**	N/A	O-EME-LIEB-060619/1105
ovation_ocr400_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	28-05-2019	6.5	In Emerson Ovation OCR400 Controller 3.3.1 and earlier, a heap-based buffer overflow vulnerability in the embedded third-party FTP server involves improper handling of a long command to the FTP service, which may cause memory corruption that halts the controller or leads to remote code execution and escalation of privileges. **CVE ID : CVE-2019-10965**	N/A	O-EME-OVAT-060619/1106
Improper Restriction of Operations within the Bounds of a	28-05-2019	6.5	In Emerson Ovation OCR400 Controller 3.3.1 and earlier, a stack-based buffer overflow vulnerability in the embedded third-party FTP server involves improper handling of a long file name from the LIST command to the FTP service, which may	N/A	O-EME-OVAT-060619/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			cause the service to overwrite buffers, leading to remote code execution and escalation of privileges. **CVE ID : CVE-2019-10967**		
Fedoraproject					
fedora					
N/A	22-05-2019	6.5	A vulnerability was found in libvirt >= 4.1.0 in the virtlockd-admin.socket and virtlogd-admin.socket systemd units. A missing SocketMode configuration parameter allows any user on the host to connect using virtlockd-admin-sock or virtlogd-admin-sock and perform administrative tasks against the virtlockd and virtlogd daemons. **CVE ID : CVE-2019-10132**	N/A	O-FED-FEDO-060619/1108
N/A	24-05-2019	6.9	It was discovered freeradius up to and including version 3.0.19 does not correctly configure logrotate, allowing a local attacker who already has control of the radiusd user to escalate his privileges to root, by tricking logrotate into writing a radiusd-writable file to a directory normally inaccessible by the radiusd user. **CVE ID : CVE-2019-10143**	https://github.com/FreeRADIUS/freeradius-server/pull/2666	O-FED-FEDO-060619/1109
Information Exposure	30-05-2019	4.7	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may	https://www.intel.com/content/www/us/en/security-center/advi	O-FED-FEDO-060619/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf **CVE ID : CVE-2019-11091**	sory/intel-sa-00233.html	
four-faith					
f3x24_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-05-2019	9	Four-Faith Wireless Mobile Router F3x24 v1.0 devices allow remote code execution via the Command Shell (aka Administration > Commands) screen. **CVE ID : CVE-2019-12168**	N/A	O-FOU-F3X2-060619/1111
Intel					
pentium_silver_n5000_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900	N/A	O-INT-PENT-060619/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
microarchitectural_data_sampling_uncacheable_memory_firmware					
Information Exposure	30-05-2019	4.7	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf **CVE ID : CVE-2019-11091**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html	O-INT-MICR-060619/1113
nuc_kit_firmware					
Improper Input Validation	17-05-2019	4.6	Insufficient input validation in system firmware for Intel (R) NUC Kit may allow an authenticated user to potentially enable escalation of privilege, denial of service, and/or information disclosure via local access. **CVE ID : CVE-2019-11094**	N/A	O-INT-NUC_-060619/1114
trusted_execution_engine_firmware					
N/A	17-05-2019	4.6	Insufficient access control	N/A	O-INT-TRUS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in Dynamic Application Loader software for Intel(R) CSME before versions 11.8.65, 11.11.65, 11.22.65, 12.0.35 and Intel(R) TXE 3.1.65, 4.0.15 may allow an unprivileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0086**		060619/1115
N/A	17-05-2019	7.2	Logic bug vulnerability in subsystem for Intel(R) CSME before version 12.0.35, Intel(R) TXE before 3.1.65, 4.0.15 may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2019-0098**	N/A	O-INT-TRUS-060619/1116
converged_security_management_engine_firmware					
N/A	17-05-2019	7.2	Logic bug vulnerability in subsystem for Intel(R) CSME before version 12.0.35, Intel(R) TXE before 3.1.65, 4.0.15 may allow an unauthenticated user to potentially enable escalation of privilege via physical access. **CVE ID : CVE-2019-0098**	N/A	O-INT-CONV-060619/1117
hns2400lp_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-HNS2-060619/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
hns2600bpb24_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1119
hns2600bpb_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1120
hns2600bpblc24_firmware					
Improper Restriction of Operations within the Bounds of a Memory	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of	N/A	O-INT-HNS2-060619/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600bpblc_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1122
hns2600bpq24_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1123
hns2600bpq_firmware					
Improper Restriction of Operations within the Bounds of a	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to	N/A	O-INT-HNS2-060619/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600bps24_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1125
hns2600bps_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1126
hns2600jf_firmware					
Improper Restriction of Operations within the Bounds	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module	N/A	O-INT-HNS2-060619/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600jff_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1128
hns2600jfq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1129
hns2600kp_firmware					
Improper Restriction of Operations within the	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System	N/A	O-INT-HNS2-060619/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600kpf_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1131
hns2600kpfr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1132
hns2600kpr_firmware					
Improper Restriction of Operations within	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server	N/A	O-INT-HNS2-060619/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
the Bounds of a Memory Buffer			Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600tp24r_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1134
hns2600tp24sr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1135
hns2600tp24str_firmware					
Improper Restriction of Operatio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable	N/A	O-INT-HNS2-060619/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ns within the Bounds of a Memory Buffer			Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600tp_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1137
hns2600tpf_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1138
hns2600tpfr_firmware					
Improper Restriction of	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family,	N/A	O-INT-HNS2-060619/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600tpnr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1140
hns2600tpr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1141
hns2600wp_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-HNS2-060619/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
hns2600wpf_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1143
hns2600wpq_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS2-060619/1144
hns7200ap_firmware					
Improper	17-05-2019	7.2	Buffer overflow vulnerability in	N/A	O-INT-HNS7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		060619/1145
hns7200apl_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS7-060619/1146
hns7200apr_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS7-060619/1147
hns7200aprl_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-HNS7-060619/1148
mfs2600ki_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-MFS2-060619/1149
mfs5000si_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-MFS5-060619/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mfs5520vir_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-MFS5-060619/1151
server_board_s1200sp_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-SERV-060619/1152
server_board_s2600bp_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access.	N/A	O-INT-SERV-060619/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0119		
server_board_s2600cw_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-SERV-060619/1154
server_board_s2600kp_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-SERV-060619/1155
server_board_s2600st_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-SERV-060619/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
server_board_s2600tp_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-SERV-060619/1157
server_board_s2600wf_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-SERV-060619/1158
server_board_s2600wt_firmware					
Improper Restriction of Operations within the Bounds of a Memory	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of	N/A	O-INT-SERV-060619/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
server_board_s7200ap_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-SERV-060619/1160
server_system_s9200wk_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-SERV-060619/1161
xeon_bronze_processors_firmware					
Improper Restriction of Operations within the Bounds of a	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to	N/A	O-INT-XEON-060619/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1163
xeon_d-1602_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1164
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1165
xeon_d-1622_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1166
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1167
xeon_d-1623n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1168
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R)	N/A	O-INT-XEON-060619/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_d-1627_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1170
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1171
xeon_d-1633n_firmware					
Improper Restriction of Operations within the Bounds of a Memory	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of	N/A	O-INT-XEON-060619/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1173
xeon_d-1637_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1174
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1175
xeon_d-1649n_firmware					
Improper	17-05-2019	7.2	Buffer overflow vulnerability in	N/A	O-INT-XEON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		060619/1176
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1177
xeon_d-1653n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1178
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a	N/A	O-INT-XEON-060619/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_d-2123it_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1180
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1181
xeon_d-2141i_firmware					
Improper Restriction of Operations within the Bounds of a Memory	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1183
xeon_d-2142it_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1184
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1185
xeon_d-2143it_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1187
xeon_d-2145nt_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1188
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially	N/A	O-INT-XEON-060619/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_d-2146nt_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1190
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1191
xeon_d-2161i_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1193
xeon_d-2163it_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1194
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1195
xeon_d-2166nt_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1197
xeon_d-2173it_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1198
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially	N/A	O-INT-XEON-060619/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_d-2177nt_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1200
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1201
xeon_d-2183it_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1203
xeon_d-2187nt_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1204
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1205
xeon_d-2191_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1207
xeon_gold_processors_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1208
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially	N/A	O-INT-XEON-060619/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_platinum_processors_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1210
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1211
xeon_processor_d-1513n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1213
xeon_processor_d-1518_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1214
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1215
xeon_processor_d-1520_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1217
xeon_processor_d-1521_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1218
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially	N/A	O-INT-XEON-060619/1219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_processor_d-1523n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1220
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1221
xeon_processor_d-1527_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1223
xeon_processor_d-1528_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1224
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1225
xeon_processor_d-1529_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1227
xeon_processor_d-1531_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1228
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially	N/A	O-INT-XEON-060619/1229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_processor_d-1533n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1230
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1231
xeon_processor_d-1537_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1233
xeon_processor_d-1539_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1234
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1235
xeon_processor_d-1540_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1237
xeon_processor_d-1541_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1238
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially	N/A	O-INT-XEON-060619/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_processor_d-1543n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1240
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1241
xeon_processor_d-1548_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1243
xeon_processor_d-1553n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1244
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1245
xeon_processor_d-1557_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1247
xeon_processor_d-1559_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1248
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially	N/A	O-INT-XEON-060619/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**		
xeon_processor_d-1567_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1250
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1251
xeon_processor_d-1571_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of	N/A	O-INT-XEON-060619/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1253
xeon_processor_d-1577_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R) Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**	N/A	O-INT-XEON-060619/1254
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1255
xeon_silver_processors_firmware					
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)	N/A	O-INT-XEON-060619/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Xeon(R) Processor D Family, Intel(R) Xeon(R) Scalable Processor, Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0119**		
N/A	17-05-2019	7.2	Insufficient access control in silicon reference firmware for Intel(R) Xeon(R) Scalable Processor, Intel(R) Xeon(R) Processor D Family may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access. **CVE ID : CVE-2019-0126**	N/A	O-INT-XEON-060619/1257
atom_230_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-ATOM-060619/1258
atom_330_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-ATOM-060619/1259
atom_x5-e3930_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-ATOM-060619/1260
atom_x5-e3940_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor	N/A	O-INT-ATOM-060619/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
atom_x7-e3950_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-ATOM-060619/1262
celeron_j3060_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900	N/A	O-INT-CELE-060619/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
celeron_j3160_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1264
celeron_j3355_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access.	N/A	O-INT-CELE-060619/1265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0120		
celeron_j3455_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1266
celeron_j4005_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1267
celeron_j4105_firmware					
Improper Access	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R)	N/A	O-INT-CELE-060619/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
celeron_n2830_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1269
celeron_n2840_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R)	N/A	O-INT-CELE-060619/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
celeron_n2930_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1271
celeron_n2940_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to	N/A	O-INT-CELE-060619/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
celeron_n3000_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1273
celeron_n3350_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1274
celeron_n3450_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1275
celeron_n4000_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-CELE-060619/1276
celeron_n4100_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor	N/A	O-INT-CELE-060619/1277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
j3710_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-J371-060619/1278
j4205_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900	N/A	O-INT-J420-060619/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
j5005_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-J500-060619/1280
n3530_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access.	N/A	O-INT-N353-060619/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0120		
n3540_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-N354-060619/1282
n5000_firmware					
Improper Access Control	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**	N/A	O-INT-N500-060619/1283
pentium_silver_j5005_firmware					
Improper Access	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R)	N/A	O-INT-PENT-060619/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor A Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access. **CVE ID : CVE-2019-0120**		
kalkitech					
sync3000_firmware					
N/A	22-05-2019	10	Kalki Kalkitech SYNC3000 Substation DCU GPC v2.22.6, 2.23.0, 2.24.0, 3.0.0, 3.1.0, 3.1.16, 3.2.3, 3.2.6, 3.5.0, 3.6.0, and 3.6.1, when WebHMI is not installed, allows an attacker to inject client-side commands or scripts to be executed on the device with privileged access, aka CYB/2019/19561. The attack requires network connectivity to the device and exploits the webserver interface, typically through a browser. **CVE ID : CVE-2019-11536**	N/A	O-KAL-SYNC-060619/1285
Linux					
linux_kernel					
NULL Pointer Dereference	27-05-2019	4.9	An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow	N/A	O-LIN-LINU-060619/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker to cause a denial of service (NULL pointer dereference and system crash). **CVE ID : CVE-2019-12378**		
N/A	27-05-2019	4.9	An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. There is a memory leak in a certain case of an ENOMEM outcome of kmalloc. **CVE ID : CVE-2019-12379**	N/A	O-LIN-LINU-060619/1287
N/A	27-05-2019	2.1	An issue was discovered in the efi subsystem in the Linux kernel through 5.1.5. phys_efi_set_virtual_address_map in arch/x86/platform/efi/efi.c and efi_call_phys_prolog in arch/x86/platform/efi/efi_64.c mishandle memory allocation failures. **CVE ID : CVE-2019-12380**	N/A	O-LIN-LINU-060619/1288
NULL Pointer Dereference	27-05-2019	4.9	An issue was discovered in ip_ra_control in net/ipv4/ip_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). **CVE ID : CVE-2019-12381**	N/A	O-LIN-LINU-060619/1289
NULL Pointer Dereference	27-05-2019	4.9	An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux kernel through 5.1.5. There is an unchecked kstrdup of fwstr, which might	N/A	O-LIN-LINU-060619/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to cause a denial of service (NULL pointer dereference and system crash). **CVE ID : CVE-2019-12382**		
Improper Input Validation	30-05-2019	7.2	An issue was discovered in wcd9335_codec_enable_dec in sound/soc/codecs/wcd9335.c in the Linux kernel through 5.1.5. It uses kstrndup instead of kmemdup_nul, which allows attackers to have an unspecified impact via unknown vectors. **CVE ID : CVE-2019-12454**	N/A	O-LIN-LINU-060619/1291
NULL Pointer Dereference	30-05-2019	4.9	An issue was discovered in sunxi_divs_clk_setup in drivers/clk/sunxi/clk-sunxi.c in the Linux kernel through 5.1.5. There is an unchecked kstrndup of derived_name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). **CVE ID : CVE-2019-12455**	N/A	O-LIN-LINU-060619/1292
Improper Input Validation	30-05-2019	7.2	An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. It allows local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_number between two kernel reads of that value, aka a "double fetch" vulnerability. **CVE ID : CVE-2019-12456**	N/A	O-LIN-LINU-060619/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Microsoft					
azure_devops_server_2019					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-05-2019	3.5	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0979. **CVE ID : CVE-2019-0872**	N/A	O-MIC-AZUR-060619/1294
Information Exposure	16-05-2019	9	An information disclosure vulnerability exists when Azure DevOps Server and Microsoft Team Foundation Server do not properly sanitize a specially crafted authentication request to an affected server, aka 'Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0971**	N/A	O-MIC-AZUR-060619/1295
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-05-2019	3.5	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0872. **CVE ID : CVE-2019-0979**	N/A	O-MIC-AZUR-060619/1296
windows_10					
N/A	16-05-2019	6.9	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it.To exploit the vulnerability, in a local attack scenario, an attacker could run a specially crafted application to elevate the attacker's privilege level, aka 'Windows NDIS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0707**		060619/1297
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0727**	N/A	O-MIC-WIND-060619/1298
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0863**	N/A	O-MIC-WIND-060619/1299
N/A	16-05-2019	4.6	A security feature bypass vulnerability exists in Windows	N/A	O-MIC-WIND-060619/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0733**		
N/A	16-05-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**	N/A	O-MIC-WIND-060619/1301
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**	N/A	O-MIC-WIND-060619/1302
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of	N/A	O-MIC-WIND-060619/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. **CVE ID : CVE-2019-0881**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**	N/A	O-MIC-WIND-060619/1304
Improper Input Validation	16-05-2019	9.3	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**	N/A	O-MIC-WIND-060619/1305
Information Exposure	16-05-2019	2.7	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0886**	N/A	O-MIC-WIND-060619/1306
Improper Restriction of Operations within the Bounds of a Memory	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-	N/A	O-MIC-WIND-060619/1307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**	N/A	O-MIC-WIND-060619/1308
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**	N/A	O-MIC-WIND-060619/1309
N/A	16-05-2019	7.2	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0892**		060619/1310
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**	N/A	O-MIC-WIND-060619/1311
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**	N/A	O-MIC-WIND-060619/1312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0895**	N/A	O-MIC-WIND-060619/1313
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0896**	N/A	O-MIC-WIND-060619/1314
Improper Restriction of Operations within the Bounds of a	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889,	N/A	O-MIC-WIND-060619/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**	N/A	O-MIC-WIND-060619/1316
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND-060619/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0899		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0900**	N/A	O-MIC-WIND-060619/1318
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902. **CVE ID : CVE-2019-0901**	N/A	O-MIC-WIND-060619/1319
Improper Restriction of Operations within the Bounds	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060619/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0903**	N/A	O-MIC-WIND-060619/1321
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0931**	N/A	O-MIC-WIND-060619/1322
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734. **CVE ID : CVE-2019-0936**	N/A	O-MIC-WIND-060619/1323
N/A	16-05-2019	2.1	An elevation of privilege vulnerability exists in the Unified Write Filter (UWF)	N/A	O-MIC-WIND-060619/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			feature for Windows 10 when it improperly restricts access to the registry, aka 'Unified Write Filter Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0942**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0882. **CVE ID : CVE-2019-0961**	N/A	O-MIC-WIND-060619/1325
windows_7					
Improper Input Validation	16-05-2019	10	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0708**	N/A	O-MIC-WIND-060619/1326
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0863**	N/A	O-MIC-WIND-060619/1327
N/A	16-05-2019	9.3	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**		060619/1328
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**	N/A	O-MIC-WIND-060619/1329
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0881**	N/A	O-MIC-WIND-060619/1330
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This	N/A	O-MIC-WIND-060619/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**		
Improper Input Validation	16-05-2019	9.3	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**	N/A	O-MIC-WIND-060619/1332
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**	N/A	O-MIC-WIND-060619/1333
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-	N/A	O-MIC-WIND-060619/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**	N/A	O-MIC-WIND-060619/1335
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**	N/A	O-MIC-WIND-060619/1336
Improper Restriction of Operatio	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in	N/A	O-MIC-WIND-060619/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ns within the Bounds of a Memory Buffer			memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0895**	N/A	O-MIC-WIND-060619/1338
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-	N/A	O-MIC-WIND-060619/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0896**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**	N/A	O-MIC-WIND-060619/1340
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**	N/A	O-MIC-WIND-060619/1341
Improper Restriction of	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine	N/A	O-MIC-WIND-060619/1342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0899**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0900**	N/A	O-MIC-WIND-060619/1343
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895,	N/A	O-MIC-WIND-060619/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902. **CVE ID : CVE-2019-0901**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**	N/A	O-MIC-WIND-060619/1345
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0903**	N/A	O-MIC-WIND-060619/1346
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734.	N/A	O-MIC-WIND-060619/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0936		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0882. **CVE ID : CVE-2019-0961**	N/A	O-MIC-WIND-060619/1348
windows_8.1					
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it.To exploit the vulnerability, in a local attack scenario, an attacker could run a specially crafted application to elevate the attacker's privilege level, aka 'Windows NDIS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0707**	N/A	O-MIC-WIND-060619/1349
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0863**	N/A	O-MIC-WIND-060619/1350
N/A	16-05-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to	N/A	O-MIC-WIND-060619/1351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**	N/A	O-MIC-WIND-060619/1352
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0881**	N/A	O-MIC-WIND-060619/1353
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**	N/A	O-MIC-WIND-060619/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-05-2019	9.3	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**	N/A	O-MIC-WIND-060619/1355
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**	N/A	O-MIC-WIND-060619/1356
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**	N/A	O-MIC-WIND-060619/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**	N/A	O-MIC-WIND-060619/1358
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**	N/A	O-MIC-WIND-060619/1359
Improper Restriction of Operations within the Bounds of a	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889,	N/A	O-MIC-WIND-060619/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0895**	N/A	O-MIC-WIND-060619/1361
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND-060619/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0896		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**	N/A	O-MIC-WIND-060619/1363
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**	N/A	O-MIC-WIND-060619/1364
Improper Restriction of Operations within the Bounds	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060619/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0899**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0900**	N/A	O-MIC-WIND-060619/1366
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902.	N/A	O-MIC-WIND-060619/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0901		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**	N/A	O-MIC-WIND-060619/1368
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0903**	N/A	O-MIC-WIND-060619/1369
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734. **CVE ID : CVE-2019-0936**	N/A	O-MIC-WIND-060619/1370
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	O-MIC-WIND-060619/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0882. **CVE ID : CVE-2019-0961**		
windows_rt_8.1					
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it.To exploit the vulnerability, in a local attack scenario, an attacker could run a specially crafted application to elevate the attacker's privilege level, aka 'Windows NDIS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0707**	N/A	O-MIC-WIND-060619/1372
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0863**	N/A	O-MIC-WIND-060619/1373
N/A	16-05-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an	N/A	O-MIC-WIND-060619/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**	N/A	O-MIC-WIND-060619/1375
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0881**	N/A	O-MIC-WIND-060619/1376
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**	N/A	O-MIC-WIND-060619/1377
Improper Input Validatio	16-05-2019	9.3	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input,	N/A	O-MIC-WIND-060619/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**	N/A	O-MIC-WIND-060619/1379
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**	N/A	O-MIC-WIND-060619/1380
Improper Restriction of Operatio	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in	N/A	O-MIC-WIND-060619/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ns within the Bounds of a Memory Buffer			memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**	N/A	O-MIC-WIND-060619/1382
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-	N/A	O-MIC-WIND-060619/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0895**	N/A	O-MIC-WIND-060619/1384
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0896**	N/A	O-MIC-WIND-060619/1385
Improper Restriction of	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine	N/A	O-MIC-WIND-060619/1386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**	N/A	O-MIC-WIND-060619/1387
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895,	N/A	O-MIC-WIND-060619/1388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0899**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0900**	N/A	O-MIC-WIND-060619/1389
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902. **CVE ID : CVE-2019-0901**	N/A	O-MIC-WIND-060619/1390
Improper Restrictio	16-05-2019	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-060619/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0903**	N/A	O-MIC-WIND-060619/1392
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734. **CVE ID : CVE-2019-0936**	N/A	O-MIC-WIND-060619/1393
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This	N/A	O-MIC-WIND-060619/1394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-0758, CVE-2019-0882. **CVE ID : CVE-2019-0961**		
windows_server_2008					
Improper Input Validation	16-05-2019	10	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0708**	N/A	O-MIC-WIND-060619/1395
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0725**	N/A	O-MIC-WIND-060619/1396
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0863**	N/A	O-MIC-WIND-060619/1397
N/A	16-05-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace	N/A	O-MIC-WIND-060619/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**	N/A	O-MIC-WIND-060619/1399
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0881**	N/A	O-MIC-WIND-060619/1400
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**	N/A	O-MIC-WIND-060619/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-05-2019	9.3	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**	N/A	O-MIC-WIND-060619/1402
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**	N/A	O-MIC-WIND-060619/1403
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**	N/A	O-MIC-WIND-060619/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**	N/A	O-MIC-WIND-060619/1405
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**	N/A	O-MIC-WIND-060619/1406
Improper Restriction of Operations within the Bounds of a	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889,	N/A	O-MIC-WIND-060619/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0895**	N/A	O-MIC-WIND-060619/1408
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND-060619/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0896		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**	N/A	O-MIC-WIND-060619/1410
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**	N/A	O-MIC-WIND-060619/1411
Improper Restriction of Operations within the Bounds	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060619/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0899**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0900**	N/A	O-MIC-WIND-060619/1413
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902.	N/A	O-MIC-WIND-060619/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0901		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**	N/A	O-MIC-WIND-060619/1415
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0903**	N/A	O-MIC-WIND-060619/1416
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734. **CVE ID : CVE-2019-0936**	N/A	O-MIC-WIND-060619/1417
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	O-MIC-WIND-060619/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0882. **CVE ID : CVE-2019-0961**		
windows_server_2012					
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it.To exploit the vulnerability, in a local attack scenario, an attacker could run a specially crafted application to elevate the attacker's privilege level, aka 'Windows NDIS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0707**	N/A	O-MIC-WIND-060619/1419
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0725**	N/A	O-MIC-WIND-060619/1420
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege	N/A	O-MIC-WIND-060619/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2019-0863**		
N/A	16-05-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**	N/A	O-MIC-WIND-060619/1422
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**	N/A	O-MIC-WIND-060619/1423
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0881**	N/A	O-MIC-WIND-060619/1424
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the	N/A	O-MIC-WIND-060619/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**		
Improper Input Validation	16-05-2019	9.3	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**	N/A	O-MIC-WIND-060619/1426
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**	N/A	O-MIC-WIND-060619/1427
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-	N/A	O-MIC-WIND-060619/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**	N/A	O-MIC-WIND-060619/1429
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**	N/A	O-MIC-WIND-060619/1430
Improper	16-05-2019	9.3	A remote code execution	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**		060619/1431
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0895**	N/A	O-MIC-WIND-060619/1432
Improper Restriction of Operations within the Bounds of a Memory	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-	N/A	O-MIC-WIND-060619/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0896**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**	N/A	O-MIC-WIND-060619/1434
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**	N/A	O-MIC-WIND-060619/1435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0899**	N/A	O-MIC-WIND-060619/1436
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0900**	N/A	O-MIC-WIND-060619/1437
Improper Restriction of Operations within the Bounds of a	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889,	N/A	O-MIC-WIND-060619/1438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902. **CVE ID : CVE-2019-0901**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**	N/A	O-MIC-WIND-060619/1439
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0903**	N/A	O-MIC-WIND-060619/1440
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege	N/A	O-MIC-WIND-060619/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0734. **CVE ID : CVE-2019-0936**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0882. **CVE ID : CVE-2019-0961**	N/A	O-MIC-WIND-060619/1442
windows_server_2016					
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it.To exploit the vulnerability, in a local attack scenario, an attacker could run a specially crafted application to elevate the attacker's privilege level, aka 'Windows NDIS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0707**	N/A	O-MIC-WIND-060619/1443
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0725**	N/A	O-MIC-WIND-060619/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0727**	N/A	O-MIC-WIND-060619/1445
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0863**	N/A	O-MIC-WIND-060619/1446
N/A	16-05-2019	4.6	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0733**	N/A	O-MIC-WIND-060619/1447
N/A	16-05-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using	N/A	O-MIC-WIND-060619/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**		
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**	N/A	O-MIC-WIND-060619/1449
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0881**	N/A	O-MIC-WIND-060619/1450
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**	N/A	O-MIC-WIND-060619/1451
Improper Input	16-05-2019	9.3	A remote code execution vulnerability exists when	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**		060619/1452
Information Exposure	16-05-2019	2.7	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0886**	N/A	O-MIC-WIND-060619/1453
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**	N/A	O-MIC-WIND-060619/1454
Improper Restriction of Operations within the Bounds of a	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889,	N/A	O-MIC-WIND-060619/1455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**	N/A	O-MIC-WIND-060619/1456
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0892**	N/A	O-MIC-WIND-060619/1457
Improper Restriction of Operations within the Bounds	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060619/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**	N/A	O-MIC-WIND-060619/1459
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND-060619/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0895		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0896**	N/A	O-MIC-WIND-060619/1461
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**	N/A	O-MIC-WIND-060619/1462
Improper Restriction of Operations within the Bounds	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-060619/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0899**	N/A	O-MIC-WIND-060619/1464
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND-060619/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0900		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902. **CVE ID : CVE-2019-0901**	N/A	O-MIC-WIND-060619/1466
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**	N/A	O-MIC-WIND-060619/1467
Improper Restriction of Operations within the Bounds	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution	N/A	O-MIC-WIND-060619/1468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			Vulnerability'. **CVE ID : CVE-2019-0903**		
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0931**	N/A	O-MIC-WIND-060619/1469
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734. **CVE ID : CVE-2019-0936**	N/A	O-MIC-WIND-060619/1470
N/A	16-05-2019	2.1	An elevation of privilege vulnerability exists in the Unified Write Filter (UWF) feature for Windows 10 when it improperly restricts access to the registry, aka 'Unified Write Filter Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0942**	N/A	O-MIC-WIND-060619/1471
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0882.	N/A	O-MIC-WIND-060619/1472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0961		
windows_server_2019					
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it.To exploit the vulnerability, in a local attack scenario, an attacker could run a specially crafted application to elevate the attacker's privilege level, aka 'Windows NDIS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0707**	N/A	O-MIC-WIND-060619/1473
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0725**	N/A	O-MIC-WIND-060619/1474
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege	N/A	O-MIC-WIND-060619/1475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2019-0727**		
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0863**	N/A	O-MIC-WIND-060619/1476
N/A	16-05-2019	4.6	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0733**	N/A	O-MIC-WIND-060619/1477
N/A	16-05-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator.The update addresses this vulnerability by changing how these requests are validated., aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0936. **CVE ID : CVE-2019-0734**	N/A	O-MIC-WIND-060619/1478
Informati on	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	O-MIC-WIND-060619/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0882, CVE-2019-0961. **CVE ID : CVE-2019-0758**		
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0881**	N/A	O-MIC-WIND-060619/1480
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0961. **CVE ID : CVE-2019-0882**	N/A	O-MIC-WIND-060619/1481
Improper Input Validation	16-05-2019	9.3	A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input, aka 'Windows OLE Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0885**	N/A	O-MIC-WIND-060619/1482
Information Exposure	16-05-2019	2.7	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information	N/A	O-MIC-WIND-060619/1483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. **CVE ID : CVE-2019-0886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0889**	N/A	O-MIC-WIND-060619/1484
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0890**	N/A	O-MIC-WIND-060619/1485
Improper Restriction of Operations within	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database	N/A	O-MIC-WIND-060619/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
the Bounds of a Memory Buffer			Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0891**		
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0892**	N/A	O-MIC-WIND-060619/1487
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0893**	N/A	O-MIC-WIND-060619/1488
Improper Restriction of Operatio	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in	N/A	O-MIC-WIND-060619/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ns within the Bounds of a Memory Buffer			memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0894**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0895**	N/A	O-MIC-WIND-060619/1490
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0897, CVE-2019-	N/A	O-MIC-WIND-060619/1491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0896**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0897**	N/A	O-MIC-WIND-060619/1492
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0898**	N/A	O-MIC-WIND-060619/1493
Improper Restriction of	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine	N/A	O-MIC-WIND-060619/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0899**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902. **CVE ID : CVE-2019-0900**	N/A	O-MIC-WIND-060619/1495
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895,	N/A	O-MIC-WIND-060619/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902. **CVE ID : CVE-2019-0901**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0889, CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901. **CVE ID : CVE-2019-0902**	N/A	O-MIC-WIND-060619/1497
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0903**	N/A	O-MIC-WIND-060619/1498
N/A	16-05-2019	6.9	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0931**	N/A	O-MIC-WIND-060619/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-05-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0734. **CVE ID : CVE-2019-0936**	N/A	O-MIC-WIND-060619/1500
N/A	16-05-2019	2.1	An elevation of privilege vulnerability exists in the Unified Write Filter (UWF) feature for Windows 10 when it improperly restricts access to the registry, aka 'Unified Write Filter Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0942**	N/A	O-MIC-WIND-060619/1501
Information Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0758, CVE-2019-0882. **CVE ID : CVE-2019-0961**	N/A	O-MIC-WIND-060619/1502
Mitsubishielectric					
qj71e71-100_firmware					
Uncontrolled Resource Consumption	23-05-2019	7.8	In Mitsubishi Electric MELSEC-Q series Ethernet module QJ71E71-100 serial number 20121 and prior, an attacker could send crafted TCP packets against the FTP service, forcing the target devices to enter an error mode and cause a denial-	N/A	O-MIT-QJ71-060619/1503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of-service condition. **CVE ID : CVE-2019-10977**		
Mobotix					
s14_firmware					
Cross-Site Request Forgery (CSRF)	31-05-2019	9.3	There is a lack of CSRF countermeasures on MOBOTIX S14 MX-V4.2.1.61 cameras, as demonstrated by adding an admin account via the /admin/access URI. **CVE ID : CVE-2019-12502**	N/A	O-MOB-S14_-060619/1504
Motorola					
m2_firmware					
Use of Externally-Controlled Format String	23-05-2019	7.5	An issue was discovered in scopd on Motorola routers CX2 1.01 and M2 1.01. There is a Use of an Externally Controlled Format String, reachable via TCP port 8010 or UDP port 8080. **CVE ID : CVE-2019-12297**	N/A	O-MOT-M2_F-060619/1505
cx2_firmware					
Use of Externally-Controlled Format String	23-05-2019	7.5	An issue was discovered in scopd on Motorola routers CX2 1.01 and M2 1.01. There is a Use of an Externally Controlled Format String, reachable via TCP port 8010 or UDP port 8080. **CVE ID : CVE-2019-12297**	N/A	O-MOT-CX2_-060619/1506
Qualcomm					
qm215_firmware					
Integer Underflow (Wrap or	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is	https://www.qualcomm.com/company/produ	O-QUA-QM21-060619/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	ct-security/bulletins#_CVE-2019-2244	
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-QM21-060619/1508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-QM21-060619/1509
Improper Restriction of	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer	https://www.codeaurora.org/secu	O-QUA-QM21-060619/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	rity-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	
sd_600_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_6-060619/1512
215_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-215_-060619/1513
mdm9206_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-MDM9-060619/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-MDM9-060619/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2245		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1516
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
mdm9607_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-MDM9-060619/1518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-MDM9-060619/1519
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1521
mdm9650_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-MDM9-060619/1522
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-MDM9-060619/1523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1525
msm8996au_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-MSM8-060619/1526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-MSM8-060619/1527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MSM8-060619/1528
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MSM8-060619/1529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
sd_820a_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_8-060619/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_8-060619/1531
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_8-060619/1532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_8-060619/1533
sd_205_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_2-060619/1534
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_2-060619/1535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_2-060619/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_2-060619/1537
sd_210_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_2-060619/1538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_2-060619/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_2-060619/1540
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_2-060619/1541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
sd_212_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_2-060619/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_2-060619/1543
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_2-060619/1544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_2-060619/1545
sd_415_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1546
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1549
sd_425_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1552
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
sd_427_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1555
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
sd_429_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1558
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1560
sd_430_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1561
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1563
sd_435_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1564
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1566
sd_439_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1567
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1569

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2247		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1570
sd_450_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_4-060619/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_4-060619/1572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1573
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_4-060619/1574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
sd_615_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_6-060619/1576
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1578
sd_616_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1579
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_6-060619/1580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1582
sd_625_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_6-060619/1584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1585
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
sd_632_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_6-060619/1588
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1590
sd_636_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1591
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_6-060619/1592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1594
sd_650_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1596
Improper	24-05-2019	4.6	Buffer overflow can occur if	https://ww	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	w.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	060619/1597
sd_652_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_6-060619/1599
Improper Restriction of	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer	https://www.codeaurora.org/secu	O-QUA-SD_6-060619/1600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	rity-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	
sda660_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SDA6-060619/1601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SDA6-060619/1602
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple	https://www.codeauro	O-QUA-SDA6-060619/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	ra.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	
sdm439_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SDM4-060619/1604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SDM4-060619/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2245		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SDM4-060619/1606
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SDM4-060619/1607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**		
sdm630_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SDM6-060619/1608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SDM6-060619/1609
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SDM6-060619/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
sdm660_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SDM6-060619/1611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SDM6-060619/1612
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-	O-QUA-SDM6-060619/1613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SDM6-060619/1614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2248		
snapdragon_high_med_2016_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SNAP-060619/1615
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SNAP-060619/1616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
mdm9150_firmware					
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 /	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MDM9-060619/1618
mdm9640_firmware					
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-	O-QUA-MDM9-060619/1619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	bulletin	
msm8909w_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-MSM8-060619/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-MSM8-060619/1621
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute,	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-	O-QUA-MSM8-060619/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439,	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-MSM8-060619/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20 **CVE ID : CVE-2019-2248**		
qcs605_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-QCS6-060619/1624
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-QCS6-060619/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-QCS6-060619/1626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-QCS6-060619/1627
sd_670_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_6-060619/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_6-060619/1629
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute,	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-	O-QUA-SD_6-060619/1630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	code-aurora-security-bulletin	
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SD_6-060619/1631
sd_675_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-	O-QUA-SD_6-060619/1632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	2245	
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SD_6-060619/1633
sd_710_firmware					
Integer Underflow (Wrap or Wraparo	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SD_7-060619/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
und)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	lletins#_CVE-2019-2244	
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_7-060619/1635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_7-060619/1636
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-	O-QUA-SD_7-060619/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	security/bulletins#_CVE-2019-2250	
sd_712_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_7-060619/1638
Integer Underflow (Wrap or Wraparo	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input	https://www.qualcomm.com/company/product-	O-QUA-SD_7-060619/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
und)			buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	security/bulletins#_CVE-2019-2245	
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_7-060619/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SD_7-060619/1641
sd_820_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_8-060619/1642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_8-060619/1643
Improper Restrictio	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to	https://www.codeauro	O-QUA-SD_8-060619/1644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operations within the Bounds of a Memory Buffer			overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	ra.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	
sd_835_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SD_8-060619/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**		
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_8-060619/1646
Double	24-05-2019	4.6	Possibility of double free issue	https://ww	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	w.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	060619/1647
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SD_8-060619/1648
sd_845_firmware					
Integer Underflo	24-05-2019	10	Possible integer underflow can happen when calculating length	https://www.qualcom	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
w (Wrap or Wraparound)			of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	m.com/company/product-security/bulletins#_CVE-2019-2244	060619/1649
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_8-060619/1650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_8-060619/1651
Improper	24-05-2019	4.6	Buffer overflow can occur if	https://ww	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	w.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	060619/1652
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SD_8-060619/1653
sd_850_firmware					
Integer Underflow (Wrap or	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is	https://www.qualcomm.com/company/produ	O-QUA-SD_8-060619/1654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	ct-security/bulletins#_CVE-2019-2244	
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_8-060619/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_8-060619/1656
Improper Restriction of	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer	https://www.codeaurora.org/secu	O-QUA-SD_8-060619/1657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	rity-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SD_8-060619/1658
sd_855_firmware					
Integer Underflow (Wrap or Wraparo	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SD_8-060619/1659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
und)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	lletins#_CVE-2019-2244	
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2245	O-QUA-SD_8-060619/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**		
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SD_8-060619/1661
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-	O-QUA-SD_8-060619/1662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	security/bulletins#_CVE-2019-2250	
sdx20_firmware					
Integer Underflow (Wrap or Wraparound)	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2244**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2244	O-QUA-SDX2-060619/1663
Integer Underflow (Wrap or Wraparo	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input	https://www.qualcomm.com/company/product-	O-QUA-SDX2-060619/1664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
und)			buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	security/bulletins#_CVE-2019-2245	
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SDX2-060619/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20 **CVE ID : CVE-2019-2248**	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SDX2-060619/1666
sm7150_firmware					
Integer Underflow (Wrap or Wraparo	24-05-2019	10	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SM71-060619/1667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
und)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2245**	lletins#_CVE-2019-2245	
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SM71-060619/1668
sxr1130_firmware					
Improper Input Validatio	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute,	https://www.qualcomm.com/company/produ	O-QUA-SXR1-060619/1669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	ct-security/bulletins#_CVE-2019-2250	
sd_8cx_firmware					
Improper Input Validation	24-05-2019	7.2	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130 **CVE ID : CVE-2019-2250**	https://www.qualcomm.com/company/product-security/bulletins#_CVE-2019-2250	O-QUA-SD_8-060619/1670
sdx24_firmware					
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD	https://www.codeaurora.org/security-bulletin/2019/04/01/april-2019-code-aurora-security-bulletin	O-QUA-SDX2-060619/1671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2247**		
Redhat					
enterprise_linux_desktop					
Use After Free	22-05-2019	9.3	Adobe Flash Player versions 32.0.0.171 and earlier, 32.0.0.171 and earlier, and 32.0.0.171 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7837**	N/A	O-RED-ENTE-060619/1672
enterprise_linux_server					
Use After Free	22-05-2019	9.3	Adobe Flash Player versions 32.0.0.171 and earlier, 32.0.0.171 and earlier, and 32.0.0.171 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7837**	N/A	O-RED-ENTE-060619/1673
enterprise_linux_workstation					
Use After Free	22-05-2019	9.3	Adobe Flash Player versions 32.0.0.171 and earlier, 32.0.0.171 and earlier, and 32.0.0.171 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code	N/A	O-RED-ENTE-060619/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-7837**		
Samsung					
scx-824_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2019	4.3	Samsung SCX-824 printers allow a reflected Cross-Site-Scripting (XSS) vulnerability that can be triggered by using the "print from file" feature, as demonstrated by the sws/swsAlert.sws?popupid=successMsg msg parameter. **CVE ID : CVE-2019-12315**	N/A	O-SAM-SCX--060619/1675
Schneider-electric					
modicon_premium_firmware					
Information Exposure	22-05-2019	5	A CWE-200: Information Exposure vulnerability exists in all versions of the Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium which could cause the disclosure of SNMP information when reading variables in the controller using Modbus. **CVE ID : CVE-2019-6806**	N/A	O-SCH-MODI-060619/1676
Improper Check for Unusual or Exceptional Conditions	22-05-2019	5	A CWE-248: Uncaught Exception vulnerability exists in all versions of the Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium which could cause a possible denial of service when writing sensitive application variables to the controller over Modbus. **CVE ID : CVE-2019-6807**	N/A	O-SCH-MODI-060619/1677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	22-05-2019	7.5	A CWE-284: Improper Access Control vulnerability exists in all versions of the Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium which could cause a remote code execution by overwriting configuration settings of the controller over Modbus. **CVE ID : CVE-2019-6808**	N/A	O-SCH-MODI-060619/1678
Improper Check for Unusual or Exceptional Conditions	22-05-2019	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause a possible Denial of Service when specific Modbus frames are sent to the controller in the products: Modicon M340 - firmware versions prior to V3.01, Modicon M580 - firmware versions prior to V2.80, All firmware versions of Modicon Quantum and Modicon Premium. **CVE ID : CVE-2019-6819**	N/A	O-SCH-MODI-060619/1679
Use of Insufficiently Random Values	22-05-2019	5	CWE-330: Use of Insufficiently Random Values vulnerability, which could cause the hijacking of the TCP connection when using Ethernet communication in Modicon M580 firmware versions prior to V2.30, and all firmware versions of Modicon M340, Modicon Premium, Modicon Quantum. **CVE ID : CVE-2019-6821**	N/A	O-SCH-MODI-060619/1680
modicon_quantum_firmware					
Informati	22-05-2019	5	A CWE-200: Information	N/A	O-SCH-MODI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on Exposure			Exposure vulnerability exists in all versions of the Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium which could cause the disclosure of SNMP information when reading variables in the controller using Modbus. **CVE ID : CVE-2019-6806**		060619/1681
Improper Check for Unusual or Exceptional Conditions	22-05-2019	5	A CWE-248: Uncaught Exception vulnerability exists in all versions of the Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium which could cause a possible denial of service when writing sensitive application variables to the controller over Modbus. **CVE ID : CVE-2019-6807**	N/A	O-SCH-MODI-060619/1682
Improper Access Control	22-05-2019	7.5	A CWE-284: Improper Access Control vulnerability exists in all versions of the Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium which could cause a remote code execution by overwriting configuration settings of the controller over Modbus. **CVE ID : CVE-2019-6808**	N/A	O-SCH-MODI-060619/1683
N/A	22-05-2019	6.4	In Modicon Quantum all firmware versions, CWE-264: Permissions, Privileges, and Access Control vulnerabilities could cause a denial of service or unauthorized modifications of the PLC configuration when using Ethernet/IP protocol.	N/A	O-SCH-MODI-060619/1684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6815		
Improper Control of Generation of Code ('Code Injection')	22-05-2019	6.4	In Modicon Quantum all firmware versions, a CWE-94: Code Injection vulnerability could cause an unauthorized firmware modification with possible Denial of Service when using Modbus protocol. **CVE ID : CVE-2019-6816**	N/A	O-SCH-MODI-060619/1685
Improper Check for Unusual or Exceptional Conditions	22-05-2019	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause a possible Denial of Service when specific Modbus frames are sent to the controller in the products: Modicon M340 - firmware versions prior to V3.01, Modicon M580 - firmware versions prior to V2.80, All firmware versions of Modicon Quantum and Modicon Premium. **CVE ID : CVE-2019-6819**	N/A	O-SCH-MODI-060619/1686
Use of Insufficiently Random Values	22-05-2019	5	CWE-330: Use of Insufficiently Random Values vulnerability, which could cause the hijacking of the TCP connection when using Ethernet communication in Modicon M580 firmware versions prior to V2.30, and all firmware versions of Modicon M340, Modicon Premium, Modicon Quantum. **CVE ID : CVE-2019-6821**	N/A	O-SCH-MODI-060619/1687
bmx-nor-0200h_firmware					
Use of Hard-coded	22-05-2019	4	A CWE-798 use of hardcoded credentials vulnerability exists in BMX-NOR-0200H with	N/A	O-SCH-BMX--060619/1688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			firmware versions prior to V1.7 IR 19 which could cause a confidentiality issue when using FTP protocol. **CVE ID : CVE-2019-6812**		
atv_imc_drive_controller_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**	N/A	O-SCH-ATV_-060619/1689
modicon_lmc058_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon	N/A	O-SCH-MODI-060619/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**		
modicon_lmc078_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**	N/A	O-SCH-MODI-060619/1691
modicon_m100_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078,	N/A	O-SCH-MODI-060619/1692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**		
modicon_m200_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**	N/A	O-SCH-MODI-060619/1693
modicon_m241_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro,	N/A	O-SCH-MODI-060619/1694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PacDrive Pro2 **CVE ID : CVE-2019-6820**		
modicon_m251_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**	N/A	O-SCH-MODI-060619/1695
modicon_m258_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2	N/A	O-SCH-MODI-060619/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6820		
pacdrive_eco_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**	N/A	O-SCH-PACD-060619/1697
pacdrive_pro2_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**	N/A	O-SCH-PACD-060619/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pacdrive_pro_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**	N/A	O-SCH-PACD-060619/1699
modicon_m340_firmware					
Use of Insufficiently Random Values	22-05-2019	5	CWE-330: Use of Insufficiently Random Values vulnerability, which could cause the hijacking of the TCP connection when using Ethernet communication in Modicon M580 firmware versions prior to V2.30, and all firmware versions of Modicon M340, Modicon Premium, Modicon Quantum. **CVE ID : CVE-2019-6821**	N/A	O-SCH-MODI-060619/1700
modicon_m221_firmware					
Missing Authentication for Critical Function	22-05-2019	6.4	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP	N/A	O-SCH-MODI-060619/1701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 **CVE ID : CVE-2019-6820**		
Tp-link					
tl-wr840n_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2019	3.5	TP-Link TL-WR840N v5 00000005 devices allow XSS via the network name. The attacker must log into the router by breaking the password and going to the admin login page by THC-HYDRA to get the network name. With an XSS payload, the network name changed automatically and the internet connection was disconnected. All the users become disconnected from the internet. **CVE ID : CVE-2019-12195**	N/A	O-TP--TL-W-060619/1702
vstracam					
c38s_firmware					
Improper Authentication	23-05-2019	10	An issue was discovered in upgrade_firmware.cgi on VStarcam 100T (C7824WIP) CH-sys-48.53.75.119~123 and 200V (C38S) CH-sys-48.53.203.119~123 devices. A remote command can be executed through a system firmware update without	N/A	O-VST-C38S-060619/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. The attacker can modify the files within the internal firmware or even steal account information by executing a command. **CVE ID : CVE-2019-12289**		
c7824wip_firmware					
Improper Authentication	23-05-2019	10	An issue was discovered in upgrade_firmware.cgi on VStarcam 100T (C7824WIP) CH-sys-48.53.75.119~123 and 200V (C38S) CH-sys-48.53.203.119~123 devices. A remote command can be executed through a system firmware update without authentication. The attacker can modify the files within the internal firmware or even steal account information by executing a command. **CVE ID : CVE-2019-12289**	N/A	O-VST-C782-060619/1704
vstracm					
c38s_firmware					
Improper Authentication	23-05-2019	7.5	An issue was discovered in upgrade_htmls.cgi on VStarcam 100T (C7824WIP) KR75.8.53.20 and 200V (C38S) KR203.18.1.20 devices. The web service, network, and account files can be manipulated through a web UI firmware update without any authentication. The attacker can achieve access to the device through a manipulated web UI firmware update. **CVE ID : CVE-2019-12288**	N/A	O-VST-C38S-060619/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c7824iwp_firmware					
Improper Authentication	23-05-2019	7.5	An issue was discovered in upgrade_htmls.cgi on VStarcam 100T (C7824WIP) KR75.8.53.20 and 200V (C38S) KR203.18.1.20 devices. The web service, network, and account files can be manipulated through a web UI firmware update without any authentication. The attacker can achieve access to the device through a manipulated web UI firmware update. **CVE ID : CVE-2019-12288**	N/A	O-VST-C782-060619/1706
Windriver					
vxworks					
Integer Overflow or Wraparound	29-05-2019	6.8	When RPC is enabled in Wind River VxWorks 6.9 prior to 6.9.1, a specially crafted RPC request can trigger an integer overflow leading to an out-of-bounds memory copy. It may allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code. **CVE ID : CVE-2019-9865**	https://www.windriver.com/feeds/wind_river_security_notices.xml	O-WIN-VXWO-060619/1707