

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

## 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 Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/1
Incorrect Type Conversi on 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/2
			CVE ID : CVE-2019-7086		
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/3

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://hel px.adobe.co m/security /products/ acrobat/aps b19-trary code execution .			
Informati on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/		A-ADO-ACRO- 060619/7		
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	D	escription	& CVE II	D	Pat	tch	NCIIP	C ID
			have an vulneral exploita arbitrary	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						
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	10	Adobe A versions earlier, 2 earlier v 2015.00 have a b vulneral exploita arbitrary	crobat a 2019.01 2017.011 ersion, a 6.30464 uffer err bility. Su tion coul	nd Read 10.20069 1.30113 and and ear cors ccessful ld lead t	ler 9 and and and clier	https:/ px.add m/sec /prod- acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	24-05-2019	5	versions earlier, 2 earlier v 2015.00 have an vulneral exploita	2019.01 2019.010 2017.011 ersion, a 6.30464 out-of-b bility. Su tion coul	11.30113 and px.d, and m/64 and earlier bounds read buld lead to sclosure.			//hel obe.co urity ucts/ at/aps	A-ADO- 060619	
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:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
CV Scoring (CVSS)		1-2	2-3	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/11
			Adobe Acrobat and Reader		
Out-of- bounds Read	24-05-2019	5	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/13
			CVE ID : CVE-2019-7025		
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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/14
CV Scoring (CVSS)	()-	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish	Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	CID
				2015.00 have an vulneral exploita arbitrary	use after oility. Su tion cou y code ex	r free ccessful ld lead t xecution	<b>0</b>	b19- 07.htm	nl		
Out-of- bounds Write	24-05-2	2019	10	earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful				https:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co curity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-2	2019	5	versions earlier, 2 earlier v 2015.00 have an vulneral exploita	Adobe Acrobat and 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:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co curity ucts/ at/aps	A-ADO- 060619	
Use After Free	24-05-2	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:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co curity ucts/ at/aps	A-ADO- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	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 Wraparo und	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/21

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/24

Weakness	Publish	Date	CVSS	D	escription	1 & CVE II	Pa	tch	NCIIF	PC ID		
Out-of- bounds Write	24-05-2	2019	10	Adobe A versions earlier, 2 earlier, 2 earlier versions of the control of the con	s 2019.0 2019.01 2017.01 version, a 6.30464 out-of-b bility. Su tion cou y code e	10.2006 0.20069 1.30113 and and ear counds w ccessful ld lead t xecution	9 and and and clier vrite o	https:/ px.add m/sed /prod acroba b19- 07.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619		
Out-of- bounds Read	24-05-2	2019	5	Adobe A versions earlier, 2 earlier v 2015.00 have an vulneral exploita informa	https:/ px.add m/sed /prod acroba b19- 07.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619					
Out-of- bounds Write	24-05-2	2019	10	versions earlier, earlier v 2015.00 have an vulneral exploita arbitrar	Adobe Acrobat and 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				//hel obe.co curity ucts/ at/aps	A-ADO- 060619		
Use After Free	24-05-2	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://hel px.adobe.co and m/security and /products/ acrobat/aps			A-ADO-ACRO- 060619/28	
CV Scoring		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

(CVSS)

Weakness	Publisl	h Date	CVSS	D	escription	a & CVE II	)	Pat	tch	NCIIP	CID
				have an vulneral exploita arbitrary	oility. Su tion cou y code ex	ccessful ld lead t xecution		07.htm	nl		
				CVE ID :							
N/A	24-05-	-2019	6.8	Adobe A versions earlier, 2 earlier v 2015.00 have a so vulneral exploita privilege	2019.01 2019.010 2017.011 ersion, a 6.30464 ecurity boility. Su tion coul	10.2006 0.20069 1.30113 and and ear oypass ccessful ld lead t ion.	9 and and and dier	https:/ px.add m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
				CVE ID : CVE-2019-7041							
NULL Pointer Derefere nce	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:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619		
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:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619		
CV Scoring S (CVSS)	Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	24-05-2019	have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .  CVE ID: CVE-2019-7044		https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/33
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/35

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish	Date	CVSS	D	escription	n & CVE II	)	Pa	tch	NCIIP	C ID
				2015.00 have an vulneral exploita information CVE ID:	out-of-b oility. Su tion cou tion disc	ounds r ccessful ld lead t closure.	ead o	b19- 07.htm	nl		
Use After Free	24-05-2	2019	9.3	Adobe A versions earlier, 2 earlier v 2015.00 have an vulneral exploitar arbitrary	2019.01 2019.010 2017.01 ersion, a 6.30464 use after bility. Su tion cou	10.2006 0.20069 1.30113 and and ear r free ccessful ld lead t	9 and and and clier	https:/ px.add m/sed /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-2	2019	4.3	versions earlier, 2 earlier v 2015.00 have an vulneral exploita	Adobe Acrobat and 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:/ px.add m/sed /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	24-05-2	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:/ px.add m/sed /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	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 Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/41
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/42

		2015.006.30464 and earlier	140	
		have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .  CVE ID : CVE-2019-7054	b19- 07.html	
24-05-2019	5	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/43
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/44
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/45
	24-05-2019	24-05-2019 5 24-05-2019 5	CVE ID: CVE-2019-7054  Adobe Acrobat and Reader versions 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  Adobe Acrobat and Reader versions 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  Adobe Acrobat and Reader 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  Adobe Acrobat and 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.	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier versions 2019.010.20069 and earlier version, and vulnerability. Successful exploitation could lead to information disclosure.  CVE ID: CVE-2019-7055  Adobe Acrobat and Reader versions 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  Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2017.011.30113 and earlier version could lead to information disclosure.  CVE ID: CVE-2019-7056  Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2017.011.30113 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.

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pa	tch	NCIIP	CID
				CVE ID :	CVE-20	19-705	57				
Out-of- bounds Read	24-05-	-2019	5	Adobe A versions earlier, 2 earlier versions earlier, 2 earlier versions have an vulneral exploitation informa	s 2019.0 2019.01 2017.01 version, a 6.30464 out-of-b bility. Su tion cou tion disc	10.2006 0.20069 1.30113 and and ear ounds r ccessful ld lead t	9 and and and rlier ead	https:/ px.add m/sed /prod acroba b19- 07.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-	-2019	5	Adobe A versions earlier, 2 earlier v 2015.00 have an vulneral exploita informa  CVE ID:	s 2019.0 2019.01 2017.01 version, a 6.30464 out-of-b bility. Su tion cou	10.2006 0.20069 1.30113 and and ear counds r ccessful ld lead t	9 and and and rlier ead	https:/ px.ado m/sec /prod acroba b19- 07.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619	
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 .		https:/ px.ado m/sec /prod acroba b19- 07.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619			
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			Adobe Acrobat and Reader versions 2019.010.20098 and earlier, 2019.010.20098 and earlier, 2017.011.30127 and /products		be.co curity ucts/	A-ADO- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30482 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/52
CV Scoring (CVSS)		1-2	2-3 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/53
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/56

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pat	tch	NCIIP	CID
			have an vulneral exploita arbitrar	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.htm	nl		
Incorrect Type Conversi on or Cast	24-05-2019	9.3	Adobe A versions earlier, 2 earlier versions earlier, 2 earlier versions at the version arbitrary CVE ID:	2019.0 2019.01 2017.01 ersion, a 6.30464 ype conf bility. Su tion cou y code e	10.2006 0.20069 1.30113 and and ear usion ccessful ld lead t	9 and and and clier	N/A		A-ADO- 060619	
Use After Free	24-05-2019	9.3	Adobe A versions earlier, 2 earlier versions earlier, 2 earlier versions and vulneral exploitae arbitrary.	2019.01 2019.01 2017.01 ersion, a 6.30464 use after bility. Su tion cou	10.2006 0.20069 1.30113 and and ear r free ccessful ld lead t	9 and and and dier	N/A		A-ADO- 060619	
Out-of- bounds Read	24-05-2019	4.3	Adobe Acrobat and Reader versions 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:/ px.ado m/sec /prod acroba b19- 07.htm	bbe.co urity ucts/ at/aps	A-ADO- 060619		
CV Scoring (CVSS)	()-1	1-2	2-3	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/63

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	07.html	
			CVE ID : CVE-2019-7075		
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/66
CV Scoring (CVSS)		1-2	2-3 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/76
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/84

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/88
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/90
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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.	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.	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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.	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.	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.	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.	.010.20100 and 010.20099 and 011.30140 and 01.30140 and 0.38 and earlier 006.30495 and 015.006.30493 we an out-of-ulnerability. loitation could ation disclosure . 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- 060619/99			
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			
CV Scoring (CVSS	()-	1-2	2-3 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, 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/104

Weakness	Publish Date	e CVSS	D	escription	n & CVE II	)	Pat	ch:	NCIIP	C ID
			2017.01 2015.00 and 201 earlier h vulneral exploita arbitrary	6.30495 5.006.30 ave a us pility. Su tion cou	and ear 0493 and e after for ccessful ld lead to xecution	rlier, d ree o	b19- 18.htm	nl		
Use After Free	22-05-2019	10	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:/ px.add m/sec /prod acroba b19- 18.htm	be.co urity ucts/ at/aps	A-ADO- 060619		
Use After Free	22-05-2019	10	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl vulneral exploita	Adobe Acrobat and Reader versions 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:/ px.add m/sec /prodi acroba b19- 18.htm	be.co urity ucts/ at/aps	A-ADO- 060619	
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html		A-ADO- 060619		
CV Scoring (CVSS)		. 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and earlier 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/110

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security	A-ADO-ACRO- 060619/117	
CV Scoring (CVSS)		1-2	2-3 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, 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/aps 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-2019-7778	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/120

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Da	te CVS		Description	n & CVE II	D	Pat	ch	NCIIP	CID
			earlier, and ear bounds Success lead to	a, 2015.00 and 201 rlier have s read vul sful explo informat	5.006.30 an out- nerabili itation o ion disc	0493 of- ty. could losure .	18.htm	nl		
Use After Free	22-05-201	9 10	version earlier, earlier, earlier, earlier, and ear vulnera exploit arbitra	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				//hel be.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	22-05-201	9 10	version earlier, earlier, earlier, earlier, and ear vulnera exploit arbitra	Adobe Acrobat and Reader versions 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				//hel be.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	22-05-201	9 10	versior earlier, earlier, earlier, earlier,	Adobe Acrobat and Reader versions 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html		ACRO- /123
CV Scoring		-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	·					tch	NCIIP	C ID
			vulnerak exploitat arbitrary <b>CVE ID</b> :	tion coul y code ex	ld lead t xecution	0				
Double Free	22-05-2019	10	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earli vulneral exploitat	earlier, 2017.011.30140 and earlier, 2017.011.30138 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				//hel obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	22-05-2019	4.3	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earli vulneral exploitat	Adobe Acrobat and Reader versions 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.					A-ADO- 060619	
Use After Free	22-05-2019	9.3	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earlivulneral exploitations.	N/A		A-ADO- 060619				
CV Scoring (CVSS)	( )-	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	Description & CVE ID					NCIIP	C ID
				CVE ID : CVE-2019-7786							
Out-of- bounds Read	22-05-	-2019	4.3	earlier, 2 earlier v 2017.01 2015.00 and 201 earlier h read vul exploitat informat	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.					A-ADO 060619	
Use After Free	22-05-	-2019	10	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earli vulneral exploitate	Adobe Acrobat and Reader versions 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.				//hel bbe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	22-05		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:/ px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of-	22-05-	-2019	5	Adobe Acrobat and Reader				https://hel		A-ADO-	ACRO-
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6				6-7 7-8		9-10

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.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/	A-ADO-ACRO- 060619/133

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 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.	acrobat/aps b19- 18.html	
			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- 060619/134
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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

3-4

2-3

1-2

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability. Successful exploitation could lead to information disclosure.  CVE ID: CVE-2019-7799  Adobe Acrobat and Reader		
Out-of- bounds Write	22-05-2019	9.3	versions 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.	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, 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

3-4

2-3

1-2

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

Weakness	Publish Date	cvss	D	escription	& CVE II	Pat	tch	NCIIP	C ID	
			lead to i	nformati	ion discl	osure.				
			CVE ID:	CVE-20	19-780	2				
Out-of- bounds Read	22-05-2019	4.3	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds 1 Successfi lead to in	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 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  Adobe Acrobat and Reader					A-ADO- 060619	
Out-of- bounds Write	22-05-2019	10	versions earlier, 2 earlier v 2017.01 version, earlier, a and earl bounds v Successf	2017.011.30138 and earlier version, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds write vulnerability.				//hel obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	22-05-2019	10	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 3 and earl vulneral exploita arbitrary	https:/ px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ nt/aps	A-ADO- 060619				
CV Scoring (CVSS)	L   -	1-2	2-3	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-2019-7805		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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
CV Scoring (CVSS)		1-2	2-3 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, 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.	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/152

Weakness	Publish Date	cvss	D	escription	a & CVE II	Pat	tch	NCIIP	CID	
			earlier, and earlier bounds Succession lead to i	b19- 18.htm	nl					
Out-of- bounds Read	22-05-2019	5	versions earlier, 2 earlier, 2 earlier, 2 earlier, 3 and earl bounds Successi lead to i	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 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					A-ADO- 060619	
Use After Free	22-05-2019	9.3	versions earlier, 2 earlier, 2 earlier, 2 earlier, 3 and earl vulneral exploita	Adobe Acrobat and Reader versions 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.					A-ADO- 060619	
Informati on Exposure	24-05-2019	7.8	Adobe A versions earlier, 2 earlier v 2015.00 have a d vulneral	https:/ px.add m/sec /prod acroba b19- 13.htm	obe.co urity ucts/ at/aps	A-ADO- 060619				
CV Scoring		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Conversi on 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish	Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	CID
				executio	n.						
				CVE ID:	CVE-20	19-782	0				
Use After Free	22-05-2	2019	7.1	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl vulneral exploita arbitrary	2019.0 2019.01 2017.01 2015.00 and 201 ier have oility. Su tion cou	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 a use af ccessful ld lead t	0 and and and and and 0493 ter free	N/A		A-ADO 060619	
Out-of- bounds Write	22-05-2	2019	9.3	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds Successfi lead to a	Adobe Acrobat and Reader versions 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.					A-ADO- 060619	
Use After Free	22-05-2	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- 060619	
CV Scoring	Scale	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10
(CVSS	)	0-1	1-2	2-5	3 3-4 4-5 5-6		0-7	7-0	0-3	3-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7823		
Improper Restrictio n of Operatio ns 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-
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	cvss	D	escription	n & CVE II	D	Pa	tch	NCIIF	PC ID
Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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, 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- 060619	
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- 060619	
Use After	22-05	-2019	9.3	Adobe Acrobat and Reader				N/A		A-ADO-	ACRO-
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			versions 2019.010.20100 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/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.	acrobat/aps b19- 18.html	
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/174

Weakness	Publis	h Date	CVSS	De	Pa	tch	NCIIP	C ID			
				earlier, a and earl bounds i Successfi lead to in	ier have read vuli ul explo nformati	an out-onerabilition condition discription	of- ty. could osure.	18.htm	nl		
Out-of- bounds Read	22-05-	-2019	5	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds a Successfilead to in	https:/ px.add m/sed /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619				
acrobat_do	C										
Improper Restrictio n of Operatio ns 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:/ px.ado m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Incorrect Type Conversi on 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:/ px.add m/sed /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	Pa	tch	NCIIF	PC ID	
			arbitrary	y code ex	ecution	١.				
			CVE ID:	CVE-20	19-708	6				
Incorrect Type Conversi on or Cast	24-05-2019	10	Adobe A versions earlier, 2 earlier versions earlier, 2 earlier versions have a ty vulneral exploitate arbitrary	2019.010 2019.010 2017.011 ersion, a 6.30464 ype confu pility. Sud tion coul y code ex	10.2006 0.20069 1.30113 nd and ear usion ccessful d lead t	9 and and and clier	https:/ px.add m/sed /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	23-05-2019	10	Adobe A versions earlier, 2 earlier v 2015.00 have an vulneral exploitar arbitrary	https:/ px.ado m/sec /prod acroba b19- 17.htm	obe.co urity ucts/ at/aps	A-ADO- 060619				
Informati on 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:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	24-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.011.30113 and				https:/ px.add m/sed /prod	be.co urity	A-ADO- 060619	
CV Scoring (CVSS)	()-	1-2	2-3	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 use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	acrobat/aps b19- 07.html	
			CVE ID : CVE-2019-7018		
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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/182
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/184
CV Scoring (CVSS)		1-2	2-3 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-2019-7021		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/185
			Adobe Acrobat and Reader		
Out-of- bounds Read	24-05-2019	5	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/187
			CVE ID : CVE-2019-7024		
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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/188
CV Scoring (CVSS)	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Da	ate CVSS	D	escription	n & CVE II	)	Pa	tch	NCIIP	CID
			have an vulnera exploita arbitrar	6.30464 use after bility. Su tion cou y code ex	r free ccessful ld lead t xecution	<b>0</b>	b19- 07.htm	nl		
Use After Free	24-05-20	19 10	versions earlier, earlier v 2015.00 have an vulnera exploita arbitrar	Adobe Acrobat and 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					A-ADO- 060619	
Out-of- bounds Write	24-05-20	19 10	versions earlier, earlier v 2015.00 have an vulnera exploita arbitrar	Adobe Acrobat and 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				//hel obe.co curity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-20	19 5	versions earlier, earlier v 2015.00 have an vulnera exploita informa	Adobe Acrobat and 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				//hel obe.co curity ucts/ at/aps	A-ADO- 060619	
CV Scoring (CVSS)		)-1 1-2	2-3	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/192
Integer Overflow or Wraparo und	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/195

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/202

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	07.html	
			CVE ID: CVE-2019-7039		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/203
			CVE ID: CVE-2019-7040		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/204
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/205
CV Scoring (CVSS)	( )-	1-2	2-3 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/208
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/209

3-4

2-3

1-2

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

Nave an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution.   CVE ID : CVE-2019-7046	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read       24-05-2019       5       versions 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.       A-ADO-ACRO-060619/210         Use After Free       24-05-2019       9.3       Adobe Acrobat and Reader versions 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://hel px.adobe.co m/security /products/acrobat/aps b19-07.html         Out-of-bounds Read       Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2017.011.30113 and earlier, 2017.011.30113 and earlier, 2017.011.30113 and earlier, 2019.010.20069 and				dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	07.html	
Use After Free  24-05-2019  9.3  Out-of-bounds Read  Pounds  Read  24-05-2019  4.3  Pounds  Versions 2019.010.20069 and earlier, 2017.011.30113 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  A-ADO-ACRO-060619/211  Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2017.011.30113 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.  A-ADO-ACRO-060619/212	bounds	24-05-2019	5	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.	px.adobe.co m/security /products/ acrobat/aps b19-	
Out-of-bounds Read  24-05-2019  A-ADO-ACRO-060619/212  versions 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.  A-ADO-ACRO-060619/212		24-05-2019	9.3	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 .	px.adobe.co m/security /products/ acrobat/aps b19-	
	bounds	24-05-2019	4.3	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.	px.adobe.co m/security /products/ acrobat/aps b19-	

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/213
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/216

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/219
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/220
			Adobe Acrobat and Reader		
Out-of- bounds Read	24-05-2019	5	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/222
			CVE ID : CVE-2019-7059	1 / 2. 1	
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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/223
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Dat	e CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	CID
			2015.00 have an vulneral exploita arbitrary	out-of-b pility. Su tion cou y code ex	ounds w ccessful ld lead t xecution	vrite o	b19- 07.htm	nl		
Out-of- bounds Read	23-05-2019	9 5	Adobe A versions earlier, 2 earlier versions of the control of the	2019.01 2019.010 2017.011 ersion, a 6.30482 out-of-b bility. Su tion cou	10.2009 0.20098 1.30127 and and ear ounds r ccessful ld lead t losure.	8 and and and dier ead	https:/ px.ado m/sec /prod acroba b19- 17.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	24-05-2019	9 10	Adobe A versions earlier, 2 earlier versions earlier, 2 earlier versions and vulnerable exploitation arbitrary.	2019.01 2019.010 2017.011 ersion, a 6.30464 use after bility. Su tion court	10.2006 0.20069 1.30113 and and ear free ccessful ld lead t	9 and and and dier	https:/ px.add m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-201	9 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:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619			
CV Scoring (CVSS)		1 1-2	2-3	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/228
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/230

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/231
Incorrect Type Conversi on 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
CV Scoring (CVSS)	()-1	1-2	2-3 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	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/237

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	07.html	
			CVE ID : CVE-2019-7074		
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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/238
			CVE ID : CVE-2019-7075		
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/240
CV Scoring (CVSS)	( )- (	1-2	2-3 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-2019-7078	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/251

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.  CVE ID: CVE-2019-7112	17.html	
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/255
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/258

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/260
Out-of- bounds Read	of- ds 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/263
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/265

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch	NCIIP	C ID
			have an vulneral exploitation	oility. Su tion cou	ccessful ld lead t		17.htn	ıl		
			CVE ID:	CVE-20	19-712	7				
Incorrect Type Conversi on or Cast	23-05-2019	10	versions earlier, 2 earlier v 2015.00 have a ty vulneral exploita arbitrary	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  Adobe Acrobat and Reader					A-ADO- 060619	
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- 060619	
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, 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- 060619	
CV Scoring (CVSS)		1-2	2-3	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-2019-7141		
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.	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.	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
CV Scoring (CVSS)	()-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Read			earlier, 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 .	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

3-4

2-3

1-2

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

Weakness	Publis	h Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
				earlier, 2 earlier, 2 earlier, 3 and earli vulneral exploitate arbitrary	2015.006  and 2015 ier have bility. Su tion coulty y code ex	5.30495 5.006.30 a use af ccessful ld lead t xecution	and 1493 ter free 0				
Use After Free	22-05	-2019	9.3	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl vulneral exploitar arbitrary	N/A		A-ADO- 060619				
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html		A-ADO- 060619	
Use After Free	22-05	-2019	10	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2	0 and and and and and	https:/ px.add m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619			
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	Pat	ch:	NCIIP	CID	
			and earl vulneral exploita arbitrar	bility. Su tion cou y code e	ccessful ld lead t xecution	0 I.				
Use After Free	22-05-2019	10	Adobe A versions earlier, a earlier versions earlier, a earlier versions earlier versions and 201 earlier be vulneral exploitation arbitrary.	https:/ px.adc m/sec /prod- acroba b19- 18.htm	be.co urity ucts/ nt/aps	A-ADO- 060619				
Use After Free	22-05-2019	10	Adobe A versions earlier, a earlier, a and earl vulneral exploita arbitrar	https:/ px.add m/sec /prod- acroba b19- 18.htm	be.co urity ucts/ nt/aps	A-ADO- 060619				
Use After Free	22-05-2019	10	Adobe A versions earlier, a earlier, a earlier, a and earl vulneral	https:/ px.adc m/sec /prod- acroba b19- 18.htm	be.co urity ucts/ nt/aps	A-ADO- 060619				
CV Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

				Description & CVE ID					tch	ITCIIF	CID
				exploita arbitrar	y code e	xecutior	1.				
				CVE ID :	CVE-20	19-776	6				
Use After Free	22-05-20	019	10	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earlivulneral exploita arbitrar; CVE ID:	https:/ px.ado m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619				
Use After Free	22-05-20	)19	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:/ px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	22-05-20	)19	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:/ px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
CV Scoring Sc (CVSS)	cale	0-1	1-2	2-3				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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security	A-ADO-ACRO- 060619/288
CV Scoring (CVSS)		1-2	2-3 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, 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/aps 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/294

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/297
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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, 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <b>9-10</b>

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/	A-ADO-ACRO- 060619/304

6-7

7-8

8-9

9-10

4-5

CV Scoring Scale

(CVSS)

0-1

1-2

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/aps 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-2019-7790	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/307
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/310

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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
CV Scoring (CVSS)	()-1	1-2	2-3 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	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.	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-
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/319
Use After Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and	https://hel px.adobe.co	A-ADO-ACRO- 060619/320
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6 95</b>	6-7 7-8	8-9 9-10

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/aps 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-2019-7806	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/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.	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/326

3-4

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	PC ID
			bounds Successf lead to it	ul explo	itation c ion discl	ould osure.				
			CVE ID :	CVE-20	19-781	1				
Out-of- bounds Read	22-05-2019	5	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds is Successful to it.	2019.01 2017.01 2017.01 2015.00 and 2015 ier have read vuli	10.2010 0.20099 1.30140 1.30138 5.30495 5.006.30 an out-onerabilititation condiscl	0 and and and and 493 of- cy. ould osure.	https:/ px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
			CVE ID :							
Out-of- bounds Read	22-05-2019	5	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds is Successful lead to in CVE ID:	2019.01 2017.01 2017.01 2015.00 and 2015 ier have read vuli	10.2010 0.20099 1.30140 1.30138 5.30495 5.006.30 an out-onerabilititation condiscl	0 and and and and 493 of- cy. ould osure.	https:/ px.adc m/sec /prod acroba b19- 18.htm	bbe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	22-05-2019	9.3	Adobe A versions earlier, 2 earlier, 2 earlier, 2 and earl vulneral exploitar arbitrary	2019.01 2019.01 2017.01 2015.00 and 2015 ier have bility. Su	10.2010 0.20099 1.30140 1.30138 5.30495 5.006.30 a use af ccessful ld lead t	0 and and and and 493 ter free	N/A		A-ADO- 060619	
CV Scoring (CVSS)		1-2	2-3	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-2019-7814		
Informati on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 13.html	A-ADO-ACRO- 060619/330
			Adobe Acrobat and Reader		
Use After Free	22-05-2019	9.3	versions 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- 060619/331
			CVE ID: CVE-2019-7817		
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, 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	22-05-2019	9.3	Adobe Acrobat and Reader	N/A	A-ADO-ACRO-
Туре			versions 2019.010.20100 and		060619/333
CV Scoring (CVSS		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <b>9-10</b>

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Conversi on 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, 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	22-05-2019	7.1	Adobe Acrobat and Reader versions 2019.010.20100 and	N/A	A-ADO-ACRO-

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 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 Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 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 Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/345
CV Scoring (CVSS)	()-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/348

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/350
agrahat va	adam		CVE ID: CVE-2019-7841		
acrobat_re	eader				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	tio hin 24-05-2019 ds	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/351

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7085		
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/352
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/354
Informati on 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/355
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Free 24-05-2019 10 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.  CVE ID : CVE-2019-7018	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free  24-05-2019  10  24-05-2019  10  24-05-2019  10  24-05-2019  10  24-05-2019  10  24-05-2019  10  24-05-2019  10  24-05-2019  10  24-05-2019  Adobe Acrobat and Reader versions and earlier, 2019.010.20069 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-2019-7018  A-ADO-ACRO 060619/356  A-ADO-ACRO 060619/356  A-ADO-ACRO 060619/357  A-ADO-ACRO 060619/358  A-ADO-ACRO 060619/358  A-ADO-ACRO 060619/358  A-ADO-ACRO 07.html  A-ADO-ACRO 060619/358  A-ADO-ACRO 07.html  A-ADO-ACRO 07.html				have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure.		
Out-of-bounds Write  24-05-2019 Improper Restrictio n of Operatio ns within the Bounds of a Managery  A-ADO-ACRO Operatio ns within the Bounds of a Managery  A-ADO-ACRO Operatio ns within the Bounds of a Managery  A-ADO-ACRO Oarlier, 2019.010.20069 and earlier, 2015.006.30464 and earlier  vulnerability. Successful exploitation could lead to arbitrary code execution .  CVE ID: CVE-2019-7019  Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2019.010.20069 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.  A-ADO-ACRO O60619/357  A-ADO-ACRO O60619/358  A-ADO-ACRO O60619/358  A-ADO-ACRO O60619/358		24-05-2019	10	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 .	px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/356
Improper Restrictio n of Operatio ns within the Bounds of a Memory  Improper Restrictio n of Operatio ns within the Bounds of a Memory  Versions 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  Versions 2019.010.20069 and https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	bounds	24-05-2019	10	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 .	px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/357
Buffer CVE ID : CVE-2019-7020	Restrictio n of Operatio ns within the Bounds of a Memory	24-05-2019	10	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 .	px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/358

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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/362

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/367
Integer Overflow or Wraparo und	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/379

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/383

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/386
CV Scoring (CVSS)		1-2	2-3 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-2019-7048		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/387
			Adobe Acrobat and Reader		
Use After Free	24-05-2019	10	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/388
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/	A-ADO-ACRO- 060619/390
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	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-2019-7052	acrobat/aps 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-2019-7053	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/391
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/393

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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  Adobe Acrobat and Reader	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/396
Out-of- bounds Read	24-05-2019	5	versions 2019.010.20069 and earlier, 2017.011.30113 and	px.adobe.co m/security /products/	A-ADO-ACRO- 060619/397
CV Scoring (CVSS)	( )- (	1-2	<b>2-3</b> 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 read vulnerability. Successful exploitation could lead to information disclosure.	acrobat/aps b19- 07.html	
			CVE ID : CVE-2019-7059		
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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/400
CV Scoring (CVSS)		1-2	2-3 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-2019-7062		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/401
			Adobe Acrobat and Reader		
Out-of- bounds Read	24-05-2019	5	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/403
			CVE ID : CVE-2019-7065	1 /2.3	
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/404
CV Scoring (CVSS)	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			2015.00 have an derefere Successf lead to a . CVE ID:	untruste ince vulr iul explo rbitrary CVE-20	ed pointonerability itation code ex	b19- 07.htm	nl			
Out-of- bounds Read	24-05-2019	5	versions earlier, 2 earlier v 2015.00 have an vulneral exploita informa	2019.01 2019.010 2017.011 ersion, a 6.30464 out-of-b bility. Su tion coul	10.2006 0.20069 1.30113 and and ear ounds re ccessful ld lead te	9 and and and lier ead	https:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Use After Free	24-05-2019	10	versions earlier, 2 earlier v 2015.00 have an vulneral exploita	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 .				//hel obe.co urity ucts/ at/aps	A-ADO- 060619	
Incorrect Type Conversi on 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- 060619	
CV Scoring (CVSS)		1-2	2-3	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-2019-7069			
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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	
			Adobe Acrobat and Reader	https://hol		
Out-of- bounds Read	24-05-2019	4.3	versions 2019.010.20069 and earlier, 2019.011.30113 and earlier version, and	https://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/411	
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10	

Weakness	Publish	Date	cvss	D	escription	n & CVE II	D	Pa	tch	NCIIP	CID
				2015.00 have an vulneral exploita informa	out-of-b pility. Su tion cou tion disc	ounds r ccessful ld lead t closure.	ead o	b19- 07.htr	nl		
Out-of- bounds Read	24-05-	2019	4.3	versions earlier, 2 earlier v 2015.00 have an vulneral exploita informa	Adobe Acrobat and Reader versions 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					A-ADO- 060619	
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 .				https:/ px.adc m/sec /prod acroba b19- 07.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619	
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html		A-ADO-ACRO-		
CV Scoring (CVSS)		0-1	1-2	2-3	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-2019-7076			
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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/415	
			CVE ID : CVE-2019-7077			
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/417	
			CVE ID: CVE-2019-7079	h++		
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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/418	
CV Scoring (CVSS)	()-	1-2	<b>2-3</b> 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 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/421
CV Scoring (CVSS)		1-2	<b>2-3</b> 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	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		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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/423
Out-of- bounds Read	23-05-2019	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/425

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/426
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/430
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/435

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	23-05-2019	have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .  CVE ID : CVE-2019-7122  Adobe Acrobat and Reader		https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/438
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/439

Dounds of a   Memory   Memor	Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pat	tch	NCIIP	C ID
A-ADO-ACRO-Out-of-bounds Read  Out-of-bounds Read  Incorrect Type Conversi on or Cast  Out-of-bounds Read  Out-of-bounds Read  Out-of-bounds Read  Out-of-bounds Read  Out-of-bounds Read  Out-of-bounds Read  Out-of-bounds Cyscoring Scale  Out-of-bounds Read  A-ADO-ACRO-O60619/442  A-ADO-ACRO-O60619/442	of a Memory			vulneral exploita arbitrar	oility. Su tion cou y code ex	ccessful ld lead t xecution	o ı.	17.htm	nl		
Out-of- bounds Read  23-05-2019 Read  23-05-2019 A-ADO-ACRO- 060619/440  23-05-2019 Read  A-ADO-ACRO- 060619/442  A-ADO-ACRO- 060619/442  A-ADO-ACRO- 060619/442  A-ADO-ACRO- 060619/442				CVE ID :	CVE-20	19-712	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 products/ have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution .  CVE ID: CVE-2019-7128  Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2017.011.30140 and earlier, 2017.011.30140 and earlier, 2017.011.30140 and earlier, 2017.011.30140 and earlier, 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .  CVS coring Scale  Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2017.011.30140 and earlier, 2017.011.30140 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 .  CVS coring Scale  Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2017.011.30140 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier plave an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .  CVE ID: CVE-2019-7140	bounds	23-05-2019	4.3	versions earlier, 2 earlier v 2015.00 have an vulneral exploita informa	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 .				bbe.co urity ucts/ at/aps	_	
Versions 2019.010.20098 and earlier, 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  Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2017.011.30140 and earlier, 2017.011.30140 and earlier, 2017.011.30138 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.  CV Scoring Scale  0.1											
Out-of-bounds Read  22-05-2019  4.3  CV Scoring Scale  Versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 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  CV Scoring Scale  0.1  1.2  2-3  3-4  4-5  5-6  6-7  7-8  8-9  9-10	Type Conversi on or	23-05-2019	10	versions earlier, 2 earlier v 2015.00 have a ty vulneral exploita arbitrary	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				obe.co urity ucts/ at/aps		
- IIII I I-X I X-4   X-4   X-5   5-6   6-7   X-8   X-9   <b>9-11</b>	bounds	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				
	CV Scoring (CVSS		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	ո & CVE II	D	Pa	tch	NCIIF	PCID
Out-of- bounds Read	22-05	-2019	4.3	Adobe A versions earlier, 2 earlier, 2 earlier, 2 and earl bounds Successified to i	s 2019.0 2019.01 2017.01 2015.00 and 201 ier have read vul ful explo nformat	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 an out- nerabilitation of	N/A		A-ADO-ACRO- 060619/443		
Out-of- bounds Read	22-05	-2019	5	Adobe A versions earlier, 2 earlier, 2 earlier, 2 and earlier, 2 and earlier bounds Successified to i	https:/ px.add m/sed /prod acroba b19- 18.htm	bbe.co curity ucts/ at/aps	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 .				N/A		A-ADO- 060619	
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	
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

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.	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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 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.	N/A	A-ADO-ACRO- 060619/451
			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	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/452

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/455

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security	A-ADO-ACRO- 060619/462

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30140 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/aps 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/468

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish	Date	CVSS	D	escriptio	n & CVE I	D	Pa	tch	NCIIP	PC ID
				Successful lead to it	nformat	ion disc	losure.				
					CVE ID : CVE-2019-7778						
N/A	22-05-2	2019	10	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bypass vexploita arbitrary	0 and and and and and 0493 ccessful o	https://px.add m/sed /prod acroba b19- 18.htm	obe.co curity ucts/ at/aps	A-ADO- 060619			
Out-of- bounds Read	22-05-2	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: px.add m/sed /prod acroba b19- 18.htm	obe.co curity ucts/ at/aps	A-ADO- 060619	
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html		A-ADO- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	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-2019-7781		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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, 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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
CV Scoring (CVSS)		1-2	2-3 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, 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://hel px.adobe.co m/security /products/	A-ADO-ACRO- 060619/478

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	ch:	NCIIP	C ID
			earlier, a and earl vulneral exploita arbitrar	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  Adobe Acrobat and Reader				nt/aps		
Out-of- bounds Read	22-05-2019	5	versions earlier, 2 earlier, 2 earlier, 2 earlier, 3 and earl bounds Successfi lead to in	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and earlier, 2015.006.30495 and earlier, and 2015.006.30493 and earlier have an out-of-bounds read vulnerability.				//hel be.co urity ucts/ nt/aps	A-ADO- 060619	
Out-of- bounds Read	22-05-2019	5	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds Successfi lead to in	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:/ px.add m/sec /prod- acroba b19- 18.htm	be.co urity ucts/ at/aps	A-ADO- 060619	
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html		A-ADO- 060619		
CV Scoring (CVSS)	( )- (	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and earlier 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/485
			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- 060619/486
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/487
CV Scoring (CVSS)	()-	1-2	2-3 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-
CV Scoring (CVSS	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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.	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://hel px.adobe.co m/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/aps 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-2019-7805	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish	Date	CVSS	D	escription	n & CVE I	D	Pa	tch	NCIIP	C ID
				bounds read vulnerability. Successful exploitation could lead to information disclosure.  CVE ID: CVE-2019-7810							
Out-of- bounds Read	22-05-2	2019	5	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds Successfilead to it.	2019.0 2019.01 2017.01 2015.00 and 201 ier have read vul ful explo nformat	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 an out- nerabili itation o	0 and and and and 0493 of- ty. could	https:/ px.ado m/sec /prod acroba b19- 18.htm	obe.co curity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	22-05-2	2019	5	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earl bounds Successfi lead to it	Adobe Acrobat and Reader versions 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:/ px.add m/sed /prod acroba b19- 18.htm	obe.co curity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	22-05-2	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:/ px.add m/sed /prod acroba b19- 18.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	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-2019-7813		
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
Informati on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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 Conversi on 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, 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30138 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 Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 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 Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/522

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publis	h Date	CVSS	D	escriptio	n & CVE I	D	Pa	tch	NCIIP	PC ID
				arbitrar	y code e	xecution	1.				
				CVE ID	CVE-20	<b>19-78</b> 3	84				
Use After Free	22-05	-2019	10	Adobe A versions earlier, 2 earlier versions 2017.01 2015.00 and 201 earlier be vulneral exploita arbitrary	s 2019.0 2019.01 2017.01 version, 1.30138 6.30495 5.006.30 have a us bility. Su tion cou y code e	10.2010 0.20099 1.30140 3 and ear 5 and ear 6 arter faccessful ld lead t	ond and and and and and and and and and a	https:/ px.add m/sed /prod acroba b19- 18.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	22-05-	-2019	5	Adobe A versions earlier, a earlier, a and earl bounds Successible de CVE ID a	s 2019.0 2019.01 2017.01 2015.00 and 201 ier have read vul ful explo nformat	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 an out- nerabili itation o	ond and and and and 493 of- ty. could losure.	https:/ px.add m/sed /prod acroba b19- 18.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	22-05-	-2019	5	Adobe A versions earlier, 2 earlier, 2 earlier, 2 and earlier, 2 and earlier, 2 lead to i	s 2019.0 2019.01 2017.01 2015.00 and 201 ier have read vul ful explo nformat	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 an out- nerabili itation o	ond and and and and 493 of- ty. could losure.	https:/ px.add m/sed /prod acroba b19- 18.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619	
CV Scoring		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	)										

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
acrobat_re	eader_dc				
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/526
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/527
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/529
CV Scoring (CVSS)	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30482 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .  CVE ID: CVE-2019-7088	b19- 17.html	
Informati on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/532
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/536

5-6

6-7

7-8

8-9

9-10

3-4

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/542
Integer Overflow or Wraparo und	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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/550

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/554
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/558
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/560
CV Scoring (CVSS)		1-2	2-3 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-2019-7047		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/563
			CVE ID : CVE-2019-7050	https://bal	
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/564
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	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 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/566
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/567

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Descript	tion & CVE II	D	Pat	tch	NCIIP	PC ID
			. CVE ID : CVE-	-2019-705	4				
Out-of- bounds Read	24-05-2019	5	Adobe Acrobate versions 2019 earlier, 2019. earlier, 2017. earlier versions 2015.006.304 have an out-outlinerability. exploitation of information decrease.	9.010.2006 010.20069 011.30113 n, and 64 and ear f-bounds r Successful could lead t lisclosure.	9 and and and clier ead	https:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-2019	5	Adobe Acroba versions 2019 earlier, 2019. earlier version 2015.006.304 have an out-o vulnerability. exploitation of information d	9.010.2006 010.20069 011.30113 n, and 64 and ear f-bounds r Successful could lead t lisclosure.	9 and and and clier ead	https:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-2019	5	Adobe Acroba versions 2019 earlier, 2019. earlier, 2017. earlier version 2015.006.304 have an out-o vulnerability. exploitation of information d	9.010.2006 010.20069 011.30113 n, and 64 and ear f-bounds r Successful could lead t lisclosure.	9 and and and dier ead	https:/ px.adc m/sec /prod acroba b19- 07.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	24-05-2019	5	Adobe Acroba versions 2019 earlier, 2019. earlier, 2017.	9.010.2006 010.20069	9 and and	https:/ px.ado m/sec /prod	be.co urity	A-ADO- 060619	
CV Scoring (CVSS)		1-2	2-3 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 read vulnerability. Successful exploitation could lead to information disclosure.	acrobat/aps b19- 07.html	
			CVE ID : CVE-2019-7058		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/572
			CVE ID : CVE-2019-7059		
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 .	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/573
			CVE ID : CVE-2019-7060  Adobe Acrobat and Reader		
Out-of- bounds Read	23-05-2019	5	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/574
CV Scoring (CVSS)		1-2	2-3 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-2019-7061		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/575
			Adobe Acrobat and Reader		
Out-of- bounds Read	24-05-2019	5	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/577
			Adobe Acrobat and Reader	https://hol	
Out-of- bounds Read	24-05-2019	5	versions 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and	https://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/578
CV Scoring (CVSS)	()-	1-2	2-3 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-2019-7065	b19- 07.html	
NULL Pointer Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/581
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7068		
Incorrect Type Conversi on 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- 060619/582
			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- 060619/583
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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/584
			CVE ID: CVE-2019-7071		
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
CV Scoring (CVSS)	()-	1-2	<b>2-3</b> 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-2019-7072		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/588
CV Scoring (CVSS)		1-2	2-3 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 Derefere nce	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps	A-ADO-ACRO- 060619/592

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 07.html	A-ADO-ACRO- 060619/595
CV Scoring (CVSS)		1-2	2-3 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-2019-7083	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/599

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/601
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/605
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	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 Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/615
Incorrect Type Conversi on 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 17.html	A-ADO-ACRO- 060619/616

Weakness	Publis	h Date	cvss	D	Description & CVE ID				tch	NCIIF	PC ID	
Out-of- bounds Read	22-05	-2019	4.3	Adobe A versions earlier, a earlier, a earlier, a and earlier, a lounds Successible do i	s 2019.0 2019.01 2017.01 2015.00 and 201 ier have read vul ful explo nformat	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 an out- nerabili itation o	0 and and and and 0493 of- ty. could	N/A		A-ADO-ACRO- 060619/617		
Out-of- bounds Read	22-05	-2019	4.3	Adobe A versions earlier, a earlier, a earlier, a and earlier, a lounds Successified to i	s 2019.0 2019.01 2017.01 2015.00 and 201 ier have read vul ful explo nformat	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 an out- nerabili itation o	0 and and and and 0493 of- ty. could	N/A		A-ADO- 060619		
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 .			versions 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html		A-ADO- 060619	
Out-of- bounds Read	22-05	-2019	6.8	Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and			versions 2019.010.20100 and N/A			A-ADO-ACRO- 060619/620		
CV Scoring (CVSS)		0-1	1-2	2-3	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, 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		
			Adobe Acrobat and Reader versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 and		
Out-of- bounds Read	22-05-2019	4.3	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- 060619/621
			CVE ID : CVE-2019-7144  Adobe Acrobat and Reader		
Out-of- bounds Read	22-05-2019	4.3	versions 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- 060619/622
			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	N/A	A-ADO-ACRO- 060619/623

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/629

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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.	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security	A-ADO-ACRO- 060619/636	
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10	

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/aps 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-2019-7772	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19-	A-ADO-ACRO- 060619/639

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30493 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/642

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publis	h Date	CVSS	D	escription	n & CVE I	D	Pa	tch	NCIIP	CID				
				Successf lead to i	nformat	ion disc	losure.								
				CVE ID :	CVE-20	19-777	7								
Out-of- bounds Read	22-05-	-2019	5	Adobe A versions earlier, 2 earlier, 2 earlier, 2 and earl bounds Successified to i	s 2019.0 2019.01 2017.01 2015.00 and 201 ier have read vul ful explo nformat	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 an out- nerabili itation o	0 and and and and 0493 of- ty. could	https:/px.adc m/sec /prod acroba b19- 18.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619					
				Adobe A											
N/A	22-05-	-2019	10	versions earlier, 2 earlier, 2 earlier, 2 earlier, 3 and earl bypass v exploita arbitrar	https:/ px.add m/sed /prod acroba b19- 18.htm	bbe.co curity ucts/ at/aps	A-ADO- 060619								
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 .				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		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		https://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html		A-ADO-ACRO- 060619/645	
CV Scoring		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10				
(CVSS)	)														

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7780		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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	versions 2019.010.20100 and earlier, 2019.010.20099 and earlier, 2017.011.30140 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://hel px.adobe.co m/security /products/ acrobat/aps b19-18.html	
Double Free	22-05-2019	10	Adobe Acrobat and Reader versions 2019.010.20100 and	https://hel px.adobe.co	A-ADO-ACRO- 060619/649
CV Scoring (CVSS)		1-2	2-3 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, 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish D	Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
				2017.01 2015.00 and 201 earlier h read vul exploitat informat	6.30495 5.006.30 ave an o nerabilit tion coul tion disc	and ear 0493 and ut-of-bo cy. Succe dd lead t losure.	lier, d ounds essful o				
Use After Free	22-05-20	019	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:/ px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619		
Out-of- bounds Read	22-05-20	019	5	versions earlier, 2 earlier, 2 earlier, 2 earlier, 2 and earli bounds in Successfi lead to in	Adobe Acrobat and Reader versions 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:/ px.add m/sec /prod- acroba b19- 18.htm	bbe.co urity ucts/ at/aps	A-ADO- 060619	
Out-of- bounds Read	22-05-20	)19	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			px.adobe.co m/security /products/ acrobat/aps arlier, 2015.006.30495 and arlier, 2015.006.30495 and arlier, 2017.011.3010 and px.adobe.co m/security /products/ acrobat/aps b19-		A-ADO- 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/658

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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-ofbounds read vulnerability. Successful exploitation could lead to information disclosure.  CVE ID: CVE-2019-7795	https://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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-	
CV Scoring (CVSS	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publis	h Date	cvss	D	escription	n & CVE I	D	Pa	tch	NCIIF	PC 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	9/665
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.				N/A		A-ADO- 060619	
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- 060619	
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- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/	A-ADO-ACRO- 060619/671

6-7

7-8

8-9

9-10

4-5

2-3

1-2

0-1

3-4

CV Scoring Scale

(CVSS)

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.	acrobat/aps b19- 18.html	
			CVE ID: CVE-2019-7806		
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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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, 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.	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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/677

Weakness	Publish Date	cvss	Desci	ription & CVE	ID	Pa	tch	NCIIP	CID
			lead to info	rmation disc	closure.				
			CVE ID : CV	VE-2019-78	12				
Out-of- bounds Read	22-05-2019	5	Adobe Acroversions 20 earlier, 201 earlier, 201 earlier, 201 earlier, and and earlier bounds rea Successful elead to info	https:/ px.add m/sed /prod acroba b19- 18.htm	bbe.co urity ucts/ at/aps	A-ADO- 060619			
Use After Free	22-05-2019	9.3	Adobe Acroversions 20 earlier, 201 earlier, 201 earlier, 201 earlier, and and earlier vulnerability exploitation arbitrary co	N/A		A-ADO- 060619			
Informati on 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:/ px.add m/sed /prod acroba b19- 13.htm	urity ucts/ at/aps	A-ADO- 060619	
Use After	22-05-2019	9.3		obat and Rea 019.010.201		N/A		A-ADO-	ACRO-
CV Scoring (CVSS)		1-2		3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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 Conversi on 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 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 Restrictio n 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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 Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Restrictio n of Operatio ns 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30493 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 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://hel px.adobe.co m/security /products/ acrobat/aps b19- 18.html	A-ADO-ACRO- 060619/696

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	Description & CVE ID					NCIIP	PC ID
			exploita arbitrary							
			CVE ID :	CVE-20	19-783	3				
Use After Free	22-05-2019	10	Adobe A versions earlier, 2 earlier, 2 earlier, 2 earlier, 3 and earl vulneral exploita arbitrary	2019.01 2019.01 2017.01 2015.00 and 2015 ier have bility. Su tion coul	10.2010 0.20099 1.30140 1.30138 6.30495 5.006.30 a use af ccessful ld lead t	0 and and and and 493 ter free	https:/ px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
			CVE ID :							
Use After Free	22-05-2019	10	versions earlier, 2 earlier v 2017.01 2015.00 and 201 earlier h vulneral exploita	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.				//hel obe.co urity ucts/ at/aps	A-ADO- 060619	
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:/ px.add m/sec /prod acroba b19- 18.htm	bbe.co urity ucts/ at/aps	A-ADO- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	Description & CVE ID				tch	NCIIP	CID
			CVE ID : CVE-2019-7836							
Out-of- bounds Read	22-05-2019	Adobe Acrobat and Reader versions 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:/px.adc m/sec /prod acroba b19- 18.htm	obe.co urity ucts/ at/aps	A-ADO- 060619	
flash_playe	er		CVEID	CVE-ZUI	J-70 <del>1</del> 1					
Out-of- bounds Read	24-05-2019	4.3	Flash Play versions: Flash Play versions: and Flash Edge and versions: have an o vulnerable exploitati informati	32.0.0.11 yer for Go 32.0.0.11 n Player fo Internet 32.0.0.11 out-of-bou ility. Succion could	4 and e cogle Chand e cor Micro Explore 4 and e cossful lead to esure.	arlier, nrome arlier, osoft er 11 arlier ad	https:/ px.ado m/sec /prod lash- player 19-06	obe.co urity ucts/f	A-ADO- 060619	
Use After Free	23-05-2019	10	32.0.0.15 32.0.0.15 32.0.0.15 use after Successfulead to ar execution	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:/ px.adc m/sec /prod lash- player 19-19	obe.co urity ucts/f	A-ADO- 060619	
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://hel px.adobe.co m/security /products/f		A-ADO-FLAS- 060619/703	
CV Scoring (CVSS)	( )- (	1-2	2-3	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.	lash- player/apsb 19-19.html	
			CVE ID: CVE-2019-7108		
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.	N/A	A-ADO-FLAS- 060619/704
			CVE ID: CVE-2019-7837		
flash_play	er_desktop_ru	ntime			
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.	https://hel px.adobe.co m/security /products/f lash- player/apsb 19-06.html	A-ADO-FLAS- 060619/705
			CVE ID : CVE-2019-7090		
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://hel px.adobe.co m/security /products/f lash- player/apsb 19-19.html	A-ADO-FLAS- 060619/706
Out-of- bounds	23-05-2019	5	Adobe Flash Player versions 32.0.0.156 and earlier,	https://hel px.adobe.co	A-ADO-FLAS- 060619/707
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	cvss	D	escription	& CVE II	D	Pat	ch.	NCIIP	C ID
Read				32.0.0.1 32.0.0.1 out-of-b vulneral exploita informa	56 and e ounds re oility. Su tion coul tion disc	arlier ha ead ccessful ld lead t losure.	ave an o	m/sec /prod lash- player 19-19	ucts/f /apsb		
Use After Free	22-05	-2019	9.3	Adobe F 32.0.0.1 32.0.0.1 32.0.0.1 use after Successf lead to a executio	71 and e 71 and e 71 and e free vuit ful explo arbitrary	arlier, arlier, a arlier ha Inerabili itation c code	nd ave a ity. could	N/A		A-ADO- 060619	_
coldfusion	l							•			
Deserializ ation of Untruste d Data	24-05	-2019	10	and earl earlier, a earlier h untruste Successf lead to a executio	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:/ px.adc m/sec /prod oldfus psb19 10.htm	be.co urity ucts/c ion/a	A-ADO- 060619	
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	24-05	-2019	4.3	and earl earlier, a earlier h scripting Successf lead to in	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				//hel be.co urity ucts/c ion/a	A-ADO- 060619	
Unrestric ted	24-05	-2019	10	ColdFusion versions Update 2 and earlier, Update 9 and			https:/ px.ado	-	A-ADO-	COLD-	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch	NCIIP	C ID
Upload of File with Dangerou s Type			earlier h restricti	ful exploi rbitrary	e upload ss vulne itation c	l rability.	m/sec /prod oldfus psb19 14.htm	ucts/c ion/a -	060619	/711
			CVE ID :	CVE-20	19-781	6				
creative_cl	loud									
Untruste d Search Path	24-05-2019	6.8	Applicat 4.7.0.40 insecure hijacking Successf lead to p	Cloud D tion (inst 0 and ear e library l g) vulner ful exploi orivilege	aller) verlier have loading rability. Itation constantion constant	re an (dll ould on.	https:/ px.add m/sec /prod reative cloud/ 19-11	be.co urity ucts/c e- 'apsb	A-ADO- 060619	_
digital_edi	tions									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	10	4.5.10.16 a heap o Successf lead to a executio	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:/ px.adc m/sec /prod Digital Editio sb19- 16.htm	urity ucts/ - ns/ap	A-ADO- 060619		
dreamwea	ver	11								
Informati on Exposure	23-05-2019	5	19.0 and insecure impleme Successful to sif smb read to stellay att	Adobe Dreamweaver versions 9.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could ead to sensitive data disclosure if smb request is subject to a elay attack. EVE ID: CVE-2019-7097			https:/ px.adc m/sec /prod dream er/aps 21.htm	be.co urity ucts/ weav sb19-	A-ADO- 060619	
indesign										
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	cvss	D	escription	a & CVE II	D	Pa	tch	NCIIP	C ID
Improper Input Validatio n	23-05-	-2019	10	Adobe In and below hyperling vulneral exploitation arbitrary.	ow have alk proces bility. Su tion cou y code es	an unsa ssing ccessful ld lead t xecution	fe o ı.	https: px.add m/sed /prod ndesig sb19- 23.htr	obe.co curity ucts/i gn/ap	A-ADO- 060619	
experience	e_mana	ger_for	ms								
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	29-05-	-2019	4.3	Adobe E Forms v have a s scripting Successified to s disclosu CVE ID	ersions of tored crops of the c	6.2, 6.3 a oss-site ability. itation o informa	could	https: px.add m/sed /prod aem- forms 19-24	obe.co curity ucts/ /apsb	A-ADO- 060619	
xd			1					•			
Improper Limitatio n of a Pathnam e to a Restricte d Directory ('Path Traversal ')	23-05-	-2019	10	Adobe X earlier h vulneral exploita arbitrar CVE ID	nave a pa pility. Su tion cou y code e	th trave ccessful ld lead t xecution	ersal o ı.	https: px.add m/sed /prod xd/ap 22.htr	obe.co curity ucts/ sb19-	A-ADO- 060619	
Improper Limitatio n of a Pathnam e to a Restricte d Directory	23-05-	-2019	10	earlier h vulneral exploita arbitrar	be XD versions 16.0 and er have a path traversal erability. Successful bitation could lead to rary code execution.  ID: CVE-2019-7106			https://hel px.adobe.co m/security /products/ xd/apsb19- 22.html		A-ADO- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description	n & CVE ID		Pat	ch:	NCIIP	CID
('Path Traversal									
shockwav	e_player								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwar versions 12.3.4.2 have a memory vulnerability. Su exploitation cou arbitrary code e CVE ID : CVE-20	204 and ea corruption ccessful ld lead to xecution.		https:/ px.adc m/sec /prod hockw apsb1 20.htm	be.co urity ucts/s vave/	A-ADO- 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	23-05-2019	10	Adobe Shockwa versions 12.3.4.2 have a memory vulnerability. Su exploitation cou arbitrary code e CVE ID : CVE-20	https:/ px.adc m/sec /prod hockw apsb1 20.htm	be.co urity ucts/s vave/	A-ADO- 060619			
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/ hockwave/ apsb19- 20.html		A-ADO- 060619	
Improper Restrictio n of Operatio ns within the CV Scoring	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:/ px.adc m/sec /prod hockw apsb1	be.co urity ucts/s vave/	A-ADO- 060619	
(CVSS)		1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Bounds			arbitrary code execution.	20.html	
of a Memory Buffer			CVE ID : CVE-2019-7101		
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/s hockwave/ apsb19- 20.html	A-ADO-SHOC- 060619/723
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/s hockwave/ apsb19- 20.html	A-ADO-SHOC- 060619/724
Improper Restrictio n of Operatio ns 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://hel px.adobe.co m/security /products/s hockwave/ apsb19- 20.html	A-ADO-SHOC- 060619/725
bridge_cc					
Improper Restrictio n of Operatio ns within	23-05-2019	10	Adobe Bridge CC versions 9.0.2 have a heap overflow vulnerability. Successful exploitation could lead to	https://hel px.adobe.co m/security /products/ bridge/aps	A-ADO-BRID- 060619/726
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
the Bounds of a Memory			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://hel px.adobe.co m/security /products/ bridge/aps b19- 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
Informati on	23-05-2019	4.3	Adobe Bridge CC versions 9.0.2 have a memory corruption	N/A	A-ADO-BRID- 060619/732
CV Scoring (CVSS)	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pa	tch	NCIII	PC ID
Exposure			vulneral exploita informa	tion cou	ld lead t					
			CVE ID : CVE-2019-7137							
Out-of- bounds Read	23-05-2019	4.3	Adobe B have an vulneral exploita informa	out-of-b bility. Su tion cou tion disc	ounds r ccessful ld lead t closure.	ead	N/A		A-ADO- 060619	
media_enc	roder		CVE ID	CVE-ZU	119-713	08				
ineuia_enc			Adobe M	Andia En	and on the	ongion	1		1	
Use After Free	22-05-2019	6.8	13.0.2 h vulneral exploita remote	as a use- bility. Su tion cou	after-fr ccessful ld lead t	ee	N/A		A-ADO-MED 060619/734	
			CVE ID :	: CVE-20	19-784	-2				
Out-of- bounds Read	22-05-2019	4.3	Adobe M 13.0.2 h read vul exploita informa CVE ID:	as an ou nerabili tion cou tion disc	t-of-bou ty. Succe ld lead t closure.	ands essful o	N/A		A-ADO- 060619	
photoshop	o_cc									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	10	earlier, a have a h vulneral exploita arbitrar	arlier, and 20.0.2 and earlier ave a heap corruption all production and could lead to bitrary code execution.			https://hel px.adobe.co m/security /products/ photoshop/ apsb19- 15.html		A-ADO- 060619	
afian										
filerun										
Improper	30-05-2019	5	FileRun	2019.05	5.21 allo	ws	N/A		A-AFI-F	ILE-
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	& CVE II	)	Pat	ch.	NCIIP	C ID
Limitatio n of a Pathnam e to a Restricte d Directory ('Path Traversal ')				images/	•	•	O			060619	/737
Improper Limitatio n of a Pathnam e to a Restricte d Directory ('Path Traversal ')	30-05-	-2019	5	FileRun css/ext- CVE ID :	ux Direc	tory List	ting.	N/A		A-AFI-F 060619	
Improper Limitatio n of a Pathnam e to a Restricte d Directory ('Path Traversal ')	30-05-	-2019	5	FileRun customiz layer Dir <b>CVE ID</b> :	zables/p rectory L	lugins/a listing.	audio_p	N/A		A-AFI-F 060619	
Apache											
Improper				The CCI	nrintony	comma	nd in				
Improper Neutraliz ation 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-' 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escriptio	n & CVE II	)	Pa	tch	NCIIP	C ID
Weakness Generatio n ('Cross- site Scripting' )  zookeeper			4.3	XSS. SSI The printended unlikely product CVE ID:  An issue ZooKeep 3.5.0-alp ZooKeep comman permiss ACLs of returns contained plaintex Digest Accordinate overload hash valuathent conseque Authent unsalted disclose for unauthent unsal	is disablateny condition website is presented as the requirement of the string. It is the Idue that is cation. A ence, if is is disable we that is is a short of the requirement of the requirement of the Idue that is is the Idue that is is a short of the rece, if is a short of the received as the	ed by demmand in pugging a resent in site.  19-022  ent in Apto 3.4.1  5.4-beta ACL()  extracted nor action ACL Id for ation Profield with a sused for	ache 3 and . any res the ode and field as ovider th the or user	https:/keepe he.org rity.ht VE-20 0201	//zoo r.apac s/secu ml#C	A-APA-: 060619	ZOOK-
jspwiki				unprivil	_		1				
Improper											
Neutraliz ation of Input During Web Page Generatio n ('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-) 060619		

(CVSS)

Weakness	Publish Date	CVSS	D	escription	& CVE II	D	Pat	tch	NCIIP	C ID
)										
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	20-05-2019	4.3	A carefu link coul vulneral JSPWiki which co hijacking	13, ion	N/A		A-APA-J 060619			
Improper Neutraliz ation of Input During Web Page Generatio n ('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-J 060619	
camel										
Improper Restrictio n of XML External Entity Referenc e ('XXE')	28-05-2019	5	contains injection (CWE-6: outdated library.' camel-xi which w	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					A-APA-0 060619	
Apachefric	ends									
xampp										
Improper Neutraliz ation 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-2 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIPO	CID
Input During Web Page Generatio n ('Cross- site Scripting' )			NOTE: This product is discontinued.  CVE ID: CVE-2019-8924				
applaudso	olutions						
applaud_h	ıcm						
Improper Neutraliz ation of Input During Web Page Generatio n ('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.></iframe.> substring.  CVE ID: CVE-2019-11033	N/A		A-APP-A 060619,	
Artifex							
ghostscrip	t						
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-0 060619,	
Atlassian							
jira							
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Informati on 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.	N/A	A-ATL-JIRA- 060619/749
Improper Neutraliz ation of Input During Web Page Generatio n ('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 Authoriza tion	22-05-2019	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		N/A	A-ATL-JIRA- 060619/751
Improper Access Control	22-05-2019 5		The CachingResourceDownloadRew riteRule 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

4-5

3-4

2-3

1-2

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 reauthenticate to pass "WebSudo" through an improper access control vulnerability.	N/A	A-ATL-JIRA- 060619/753
• • •			CVE ID : CVE-2019-8443		
Atutor					
Unrestric ted Upload of File with Dangerou s Type	17-05-2019	9	ATutor through 2.2.4 is vulnerable to arbitrary file uploads via the mods/_core/backups/upload.p hp (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_pro	otocol_stack_p	roject			
bacnet_pro	otocol_stack				
Out-of-	30-05-2019	5	BACnet Protocol Stack through	N/A	A-BAC-BACN-
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publish D	ate CVSS	D	escription	a & CVE II	)	Pat	tch	NCIIP	C 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		<u>,</u>								
blogifier										
Improper Input Validatio n	22-05-20	19 7.5	Blogifier does not as demo checks f	t properl instrated	ly restrion I by miss pathnan	ct APIs, sing ne.	N/A		A-BLO-F 060619	
bluecats										
bc_reveal										
N/A	22-05-20	19 4.3	BlueCats stores th passwor base64 o clear tex cache ev This can compror BlueCats impleme would fi physical device o	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.					A-BLU-I 060619	_
blueprism										
robotic_pr	ocess_aut	omation								
N/A	24-05-20	19 6.5	In AutomateAppCore.dll in Blue Prism Robotic Process					A-BLU-ROBO- 060619/758		
CV Scoring (CVSS)		0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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	S Description & CVE ID					tch	NCIIP	CID
patrol_age	nt									
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- 060619	
boostio										
boostnote										
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	19-05-2019	3.5	There is XSS in browser/components/Markdo wnPreview.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.				N/A		A-B00- 060619	
bosch										
building_ii	ntegration_sys	stem								
Improper Restrictio n of Operatio ns 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://dia.bo curity/ fs/me/ b/secu advisor	schse .com/ dia/p urity_ ories/	A-BOS-I 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Da	ate CVSS	D	escription	n & CVE I	D	Pa	tch	NCIIP	C ID
of a Memory Buffer			network	2019- 0403h 2019- 6957_ ty_adv _softw uffer_u	securi risory rare_b overfl					
Improper Access Control	29-05-203	19 6.4	vulneral Video M (BVMS) DIVAR I 7000, Co Building (BIS) wi Professi Access F Bosch V Video SI network without authent respecti issue. Th "CWE-2 Control. example attacker	code in the system via the network interface.  CVE ID: CVE-2019-6957  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.				//me schse .com/ dia/p urity_ ories/ - ot-cve- securi risory oper_ c_cont f	A-BOS-1 060619	
bosch_vide	eo_manage	ement_syst					https:	//ma		
Improper Restrictio n of	29-05-202	19 7.5	A recently discovered security vulnerability affects all Bosch Video Management System				https: dia.bo curity	schse	A-BOS-1 060619	
CV Scoring (CVSS)		)-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Coperation   Swithin   S	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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.  A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) without, and below, https://me dia.boschse curity.com/ fs/media/p b/security_advisories/ bosch-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-0404bt-cve-2019-	ns within the Bounds of a Memory			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	b/security_ advisories/ bosch- 2019- 0403bt-cve- 2019- 6957_securi ty_advisory _software_b uffer_overfl	
	Access	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.	dia.boschse curity.com/ fs/media/p b/security_ advisories/ bosch- 2019- 0404bt-cve- 2019- 6958_securi ty_advisory _improper_ access_cont	

Weakness	Publish Date	CVSS	Description & CVE ID			)	Pat	tch	NCIIP	CID
Buildbot										
buildbot										
Improper Authentic ation	23-05-2019	5	Buildboth before 2 submitted from OA authenticattacker them to a victim, victim.	N/A		A-BUI-E 060619				
CA										
risk_authentication										
Informati on 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:/port.ca /us/pi t- conter omme readin urity- notice 20190 01 securi notice ca-risk auther on-and strong auther on.htm	a.com roduc nt/rec nded- g/sec s/CA 523- ty- -for- x- nticati d-ca- g- inticati	A-CA-RI 060619			
N/A	28-05-2019	6.5	vulneral adminis CA Tech Authent	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://sup port.ca.com /us/produc t- content/rec ommended-		SK- /767
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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/sec urity- notices/CA 20190523- 01 security- notice-for- ca-risk- authenticati on-and-ca- strong- authenticati on.html	
strong_aut	thentication				
Informati on 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://sup port.ca.com /us/produc t- content/rec ommended- reading/sec urity- notices/CA 20190523- 01 security- notice-for- ca-risk- authenticati on-and-ca- strong- authenticati on.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://sup port.ca.com /us/produc t- content/rec ommended- reading/sec	A-CA-STRO- 060619/769
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escription	a & CVE II	D	Pat	tch	NCIIP	C 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- notice 20190 01 securi notice ca-risk auther on-and strong auther on.htm	tyforticati d-caticati		
carts.guru										
carts_guru										
Deserializ ation of Untruste d Data	20-05-2019	7.5	The Cart WordPr Deserial source c cartsgur CVE ID:	ess allov ization v ookie to ru-event	vs Insect via a cart classes, -handler	ure tsguru- /wc- :.php.	N/A		A-CAR-0 060619	
centos-we	bpanel									
centos_we	b_panel									
Improper Neutraliz ation of Input During Web Page Generatio n ('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-0 060619	
Citrix										
receiver								1		
Improper Access Control	22-05-2019	7.5	Citrix Workspace App before 1904 for Windows has Incorrect Access Control.				N/A		A-CIT-R 060619	
CV Scoring (CVSS)		1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publis	h Date	cvss	D	escriptio	n & CVE I	D	Pa	tch	NCIIP	C ID
				CVE ID	: CVE-20	19-116	34				
commsy											
commsy											
Improper Neutraliz ation of Special Elements used in an SQL Comman d ('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 via the cid parameter. xed in 9.2.			/773
computrol	ls										
computrol	computrols_building_automation_software										
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	23-05	-2019	4.3	Unauthe Cross-Si vulneral and pass the user	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	
Cross- Site Request Forgery (CSRF)	24-05	-2019	6.8	Cross-Si	Computrols CBAS 18.0.0 allows Cross-Site Request Forgery.  CVE ID: CVE-2019-10847			N/A		A-COM- COMP- 060619	
Informati on Exposure	24-05	-2019	5	Comput Usernan	ne Enum	eration		N/A		A-COM- COMP- 060619	
Informati on Exposure	23-05	-2019	5	Computrols CBAS 18.0.0 allows unprotected Subversion (SVN) directory / source code			N/A		A-COM- COMP- 060619		
CV Scoring (CVSS)		0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			disclosure.  CVE ID : CVE-2019-10849		
Use of Hard- coded Credentia ls	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 Neutraliz ation of Special Elements used in an SQL Comman d ('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 Authentic ation	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 Neutraliz ation of Special Elements used in a Comman d ('Comma nd 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
Informati on	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 Neutraliz ation of Input During Web Page Generatio n ('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 Neutraliz ation of Input During Web Page Generatio n ('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						
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10						

Weakness	Publish Date	cvss	Description & CV	E ID	Pat	ch	NCIIP	C ID
site Scripting' )								
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 t allows remote attacke bypass access restricti browse unauthorized the application 'Manag Basic System'.	rs to on to pages via gement of	N/A		A-CYB-0 060619	
Improper Input Validatio n	17-05-2019	5.5	Cybozu Garoon 4.0.0 to allows authenticated at to alter the information privileges invoking the via unspecified vectors.  CVE ID: CVE-2019-59	nttackers n with e installer s.	N/A		A-CYB-0 060619	
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	17-05-2019	3.5	Cross-site scripting vulnerability in Cyboz 4.6.0 to 4.6.3 allows reauthenticated attacker inject arbitrary web so HTML via the applicat 'Portal'.  CVE ID: CVE-2019-59	N/A		A-CYB-0 060619		
Improper Access Control	17-05-2019	4	Cybozu Garoon 4.0.0 the allows remote authenticated attackers to bypass accrestriction to view the Board without view provide the application 'But CVE ID: CVE-2019-59	cicated cess Bulletin rivileges lletin'.	N/A		A-CYB-GARO- 060619/790	
Improper Neutraliz ation of Special Elements	17-05-2019	6.5	SQL injection vulneral the Cybozu Garoon 4.0 4.10.0 allows attacker administrator rights to arbitrary SQL comman	0.0 to with execute	N/A		A-CYB-0	
CV Scoring (CVSS)		1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	CID
used in an SQL Comman d ('SQL Injection'			the Log applicat CVE ID :							
Improper Access Control	17-05-2019	4	Cybozu allows r attacker restricti informa privilego of User I	N/A		A-CYB-0				
Improper Limitatio n of a Pathnam e to a Restricte d Directory ('Path Traversal ')	17-05-2019	5.5	Director vulneral 4.0.0 to authenti obtain fi privilego 'Work F	N/A		A-CYB-0 060619				
Improper Neutraliz ation of Input During Web Page Generatio n ('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-0 060619	
Improper Neutraliz ation 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	
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pa	tch	NCIIF	C ID
During Web Page Generatio n ('Crosssite Scripting' )			applicat	pt or HT ion 'Mail <b>CVE-20</b>	<b>'</b> .					
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	17-05-2019	4.3	Cross-sit vulneral 4.0.0 to attacker web scri applicat CVE ID:	N/A		A-CYB-0				
Improper Neutraliz ation of Input During Web Page Generatio n ('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-0	
Improper Access Control	17-05-2019	4	Cybozu ( allows re attacker restriction without the appl CVE ID :	ated ss ort s via port'.	N/A		A-CYB-0			
Improper Access Control	17-05-2019	4	Cybozu ( allows re attacker restricti	ithentic ass acce	ated ss	N/A		A-CYB-GARO- 060619/799		
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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'.	N/A	A-CYB-GARO- 060619/800
			CVE ID : CVE-2019-5943		
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 Redirecti on to Untruste d 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
CV Scoring (CVSS)	( )-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	D	Description & CVE ID				tch	NCIIF	CID
ation of Input During Web Page Generatio n ('Crosssite Scripting' )				4.6.0 to authent inject ar HTML v 'Cabinet CVE ID	to pt or n						
deltek											
maconomy	У										
Improper Limitatio n of a Pathnam e to a Restricte d Directory ('Path Traversal ')	24-05-	-2019	7.5	Deltek M prone to absolute WS.mac PATH_IN by a cgi- bin/Mac macx1.V URI.	o local file e path tr x1.W_M NFO, as o conomy, V_MCS/,	e inclus aversal i CS/ lemonst /Macono /etc/pas	ion via in the crated omyWS.	N/A		A-DEL- 060619	
digitaldrui	id										
hoteldruid	l										
Improper Neutraliz ation of Input During Web Page Generatio n ('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-I 060619	
dollarshav	eclub										
shave											
Improper	24-05-	-2019	4.3	XSS exis	ts in Sha	ve befo	re 2.5.3	N/A		A-DOL-	SHAV-
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE I	D	Pa	tch	NCIIF	PCID
Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )				because mishand overwri CVE ID :			060619	9/807			
Dotcms											
dotcms											
Improper Limitatio n of a Pathnam e to a Restricte d 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- 060619	
Drupal											
drupal											
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' ) Improper	16-05-		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  In PrestaShop 1.7.5.2, the				N/A		A-DRU- 060619 A-DRU-	9/809
Neutraliz ation of	24-05	-2019	4.3	shop_country parameter in the install/index.php installation				N/A		060619	
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generatio n ('Crosssite 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_p  dynmap	roject				
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.jav a, 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	e				
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	Publis	h Date	cvss	S Description & CVE ID					tch	NCIIP	C ID
				it with a	malicio	us app.					
				CVE ID:	<b>CVE-20</b>	19-562	5				
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-II 060619	
elabftw											
elabftw	elabftw										
Improper Neutraliz ation of Special Elements used in a Comman d ('Comma nd Injection' )	19-05-	-2019	9	eLabFTW 1.8.5 is vulnerable to arbitrary file uploads via the /app/controllers/EntityControl ler.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.				N/A		A-ELA-I 060619	
Enigmail											
enigmail											
Improper Verificati on of Cryptogr aphic 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-E 060619		
CV Scoring (CVSS)		0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch:	NCIIP	C ID
falco										
falco										
Use After Free	17-05-2019	2.1	An issue Falco the indicato resource bypass t	rough 0. r for insues allows he detec	14.0. A r ufficient clocal us tion eng	missing sers to gine.	N/A		A-FAL-F 060619	
Fasterxml										
jackson-da	ntabind									
Informati on 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.MiniA dmin validation.				N/A		A-FAS-J. 060619	
firejail_pro	oject									
firejail										
Improper Input Validatio n	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-F 060619		
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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					
Untruste d 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://fort iguard.com /advisory/F G-IR-19- 060	A-FOR-FORT- 060619/819
Freedeskt	ор				
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				
CV Scoring (CVSS		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
freeimage					
Improper Restrictio n of Operatio ns 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
Uncontro lled Resource Consump tion	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
Uncontro lled Resource Consump tion	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	In FreeImage 3.18.0, an out-of-bounds access occurs because of mishandling of the OpenJPE j2k_read_ppm_v3 function in j2k.c. The value of l N ppm		N/A	A-FRE-FREE- 060619/824

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	CID
Freeradius	S									
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:/ ub.cor eRADI eeradi server /2666	n/Fre US/fr us- r/pull	A-FRE-I 060619	
F-secure	F-secure									
psb_works	station_securi	ty								
N/A	17-05-2019	6.8	Secure S before 1 Security Anti-Vir Secure C and Pred Secure F Security Secure C Standard 19.3, a lo their pri hijacking installer the file r C:\Wind executes then atte DLLs fro	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		https:/ w.f- secure /en/w bs_glo c-2019	e.com reb/la bal/fs	A-F-S-P: 060619	_	
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	sh Date	CVSS	Description & CVE ID				Pat	:ch	NCIIP	CID
				attacker can create a malicious C:\Windows\Temp\OLEACC.dl l file. When an admin runs the installer, rm.exe will execute the attacker's DLL in an elevated security context.							
				CVE ID :	CVE-20	19-116	44				
gatship											
web_modu	ıle										
Informati on Exposure	17-05	-2019	5	1.30 allo obtain p informat ws/gats	GAT-Ship Web Module through 1.30 allows remote attackers to obtain potentially sensitive information via {} in a ws/gatshipWs.asmx/SqlVersio n request.					A-GAT-\ 060619	_
				CVE ID : CVE-2019-12163							
getbukkit											
spigot											
Improper Access Control	28-05	-2019	5	In Webb beta-3, v to a miss servlet/1 a, an atta image w enabled	vith Spig sing logi MapStor acker ca ithout lo	got 1.13. n check ageHan n see a n ogin des	2, due in dler.jav nap pite an	N/A		A-GET-S 060619	
				CVE ID :	CVE-20	19-123	95				
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-0 060619		
CV Scoring		0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	
(CVSS)	<u> </u>										

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	Publis	h Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				themes of Exploiting necessaring file is ignored factor is check or saving the assumption content creation executal content.  CVE ID:	ng the tr ry becau nored. A that the n the extens ne file, we cion that is safe. T of web a	aversal is the .h contribute isn't a ension be the para chis allowancessib with arb	taccess uting another refore ameter ws the le and itrary				
gitea											
gitea											
Improper Access Control	31-05	-2019	5	earlier d trusted i attacker access to Jenkinsf configur	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.		N/A		A-GIT-G 060619		
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-G 060619	
Uncontro lled 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			e	N/A		A-GIT-G 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	3-4 4-5 5-6			7-8	8-9	9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		11.9.x before 11.9.2. Making concurrent GET /api/v4/projects/ <id>/languag es requests may allow Uncontrolled Resource Consumption.</id>		
		CVE ID : CVE-2019-10113		
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
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
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
	16-05-2019	16-05-2019 4	16-05-2019  11.9.x before 11.9.2. Making concurrent GET /api/v4/projects/ <id> 11.9.x before 11.9.2. Making concurrent GET /api/v4/projects/<id> 10-05-2019  16-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  10-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-2019  11-05-</id></id>	11.9.x before 11.9.2. Making concurrent GET /api/v4/projects/ <id>  </id>

Weakness	Publis	h Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	PCID	
				CVE ID :	CVE-20	19-101	16					
URL Redirecti on to Untruste d Site ('Open Redirect')	16-05	-2019	5.8	An Oper discover Commune Edition before 1 11.9.2. A after such within the Second Commune Commu	red in Gi nity and before 1 1.8.4, ar A redirect ccessful he GeoAuth ndary G	tLab Enterpr 1.7.8, 11 ad 11.9.x et is trigg authenti aControl eo node	rise 8.x before gered cation ler for	N/A		A-GIT-GITL- 060619/836		
				CVE ID :								
Improper Access Control	17-05	-2019	6.4	issue wa Commun Edition ( 11.3.11, and 11.5 issue con allow a vi issue wh allowed	on Incorrect Access Control asue was discovered in GitLab ommunity and Enterprise dition 6.0 and later but before 1.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. The asue comments feature could allow a user to comment on an asue which they shouldn't be allowed to.  EVE ID: CVE-2019-5883					A-GIT-GITL- 060619/837		
Improper Neutraliz ation of Special Elements in Output Used by a Downstre am Compone nt ('Injectio n')	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-0 060619		
Improper Access Control	17-05	-2019	4	An Incorrect Access Control issue was discovered in GitLab Community and Enterprise				N/A		A-GIT-0 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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
Informati on 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,	N/A	A-GIT-GITL- 060619/843
Uncontro lled Resource Consump tion	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).	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 Validatio n	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
Informati on 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
glyphandc	no		CVE ID . CVE-2017-7000		
xpdfreade					
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	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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
Gnome	Publis	n Date	CVSS	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				Pat	cn	NCIIP	CID
gvfs											
N/A	29-05-	-2019	7.5	GNOME 1.41.2. daemon mishand because	An issue was discovered in GNOME gyfs 1.29.4 through 1.41.2. daemon/gyfsbackendadmin.c mishandles file ownership because setfsuid is not used.  CVE ID: CVE-2019-12447					A-GNO- 060619	
Concurre nt Execution using Shared Resource with Improper Synchron ization ('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- 060619		
N/A	29-05-	-2019	10	An issue was discovered in GNOME gyfs 1.29.4 through 1.41.2. daemon/gyfsbackendadmin.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- 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	& CVE II	D	Pa	tch	NCIIP	C ID	
				file:// U privilege CVE ID:	es are un	availab	le.					
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			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.				A-GNO- 060619	
GNU												
wget												
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.5	1.20.1 and remote a denial-o execute unspecif	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		
gohttp_pro	oject											
gohttp												
Improper Restrictio n of Operatio ns 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- 060619			
Out-of- bounds	17-05	-2019	5	GoHTTP through 2017-07-25 has a stack-based buffer over-			N/A		A-GOH-	GOHT-		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

called from getRequestType) via a long URL.  CVE ID: CVE-2019-12159  GoHTTP through 2017-07-25 has a sendHeader use-after-free.  CVE ID: CVE-2019-12160  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  Golang  crypto  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 Headers. The "Hash" Armor Headers 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	Weakness	Publish	n Date	cvss	De	Description & CVE ID		Pat	tch	NCIIP	C ID	
Golang  Typto  A message-forgery issue was discovered in crypto/penpsp/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 pecifies the message digest algorithm (s) used for the signature was generated using a different message digest algorithm than what was actually used. Moreover, since	Read				called fr	om getR		•			060619	/858
A-GOH-GOHT- free					CVE ID:	<b>CVE-20</b>	19-121	59				
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  A message-forgery issue was discovered in crypto/openpgp/clearsign/clea rsign.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 Headers. The "Hash" Armor Headers 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	Use After Free	17-05-	2019	7.5	has a ser	has a sendHeader use-after- free.						
there is a stack-based buffer over-read via a long User-Agent header.  CVE ID: CVE-2019-12198  A message-forgery issue was discovered in crypto/openpgp/clearsign/clea rsign.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 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					CVE ID:	CVE-20	19-121	60				
A message-forgery issue was discovered in crypto/openpspy/clearsign/clea rsign.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	Out-of- bounds Read	20-05-	2019	5	there is a stack-based buffer over-read via a long User-Agent header.				N/A			
A message-forgery issue was discovered in crypto/openpgp/clearsign/clea rsign.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	Colong				CVE ID:	CVE-ZU	19-121	90				
A message-forgery issue was discovered in crypto/openpgp/clearsign/clea rsign.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												
discovered in crypto/openpgp/clearsign/clea rsign.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	Стурго				A messa	A message-forgery issue was						
CV Scoring Scale 0.1 1.2 2.3 3.4 4.5 5.6 6.7 7.9 9.0 0.10	N/A	22-05-	2019	4.3	discover crypto/crsign.go cryptogr 03-25. A OpenPG specificate chapter message more op Headers Headers digest al signatur clearsign value of allows a Consequence of the consequence of	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 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						
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	_		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the 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 Wraparo und	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-G00-CHR0- 060619/863
Integer Overflow or Wraparo und	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-G00-CHR0- 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	cvss	D	Description & CVE ID				tch	NCIIF	PC ID	
Wraparo und				prior to remote a arbitrary via a cra	attacker y code ii fted HT	to exect nside a s ML page	ite andbox					
Incorrect Type Conversi on or Cast	23-05	-2019	6.8	V8 in Go 73.0.368 attacker bounds crafted I	priate o ogle Chi 33.75 all to perfo memory HTML pa	E-2019-5791				A-G00-CHR0 060619/866		
Integer Overflow or Wraparo und	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-G00-CHR0- 060619/867		
Improper Input Validatio n	23-05	-2019	4.3	in extension remote a extension interface page.	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			N/A		A-G00- 060619		
Improper Input Validatio n	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-G00- 060619		
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		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Wraparo und			attacker to potentially perform out of bounds memory access via a crafted PDF file.  CVE ID: CVE-2019-5795		
Concurre nt Execution using Shared Resource with Improper Synchron ization ('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	A-G00-CHR0- 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-G00-CHR0- 060619/872
Improper Input Validatio n	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-G00-CHR0- 060619/873
Improper Input Validatio n	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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	1	NCIIP	C ID
			CVE ID : CVE-2019-5800				
Improper Input Validatio n	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-G00- 060619	
Improper Input Validatio n	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-G00- 060619	
Improper Input Validatio n	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-G00- 060619	
Improper Neutraliz ation of Special Elements used in a Comman d ('Comma nd 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-G00- 060619	
gpac							
gpac							
NULL	30-05-2019	4.3	An issue was discovered in	N/A		A-GPA-0	GPAC-
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6 262</b>	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch:	NCIIP	C ID
Pointer Derefere nce			GPAC 0.7 pointer of function isomedia demonstrates CVE ID :	derefere GetESD a/track.o trated by	nce in that at in libgy MP4Bo	ne oac.a, as ox.			060619	/879
NULL Pointer Derefere nce	30-05-2019	5	An issue GPAC 0.2 pointer of function gf_isom_pe at iso libgpac.a MP4Box	JLL ne mat_ty nple.c in ed by	N/A		A-GPA-0 060619			
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	30-05-2019	6.8	GPAC 0.1 based bu function ReadGF_tification odf/ipm as demo	An issue was discovered in GPAC 0.7.1. There is a heap-based buffer overflow in the function ReadGF_IPMPX_RemoveToolNo tificationListener in odf/ipmpx_code.c in libgpac.a, as demonstrated by MP4Box.  CVE ID: CVE-2019-12483					A-GPA-0 060619	
gpg-pgp_p	roject									
gpg-pgp										
Improper Verificati on of Cryptogr aphic 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-0 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to 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 Wraparo und	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/do cs/CVE- 2019- 5435.html	A-HAX-CURL- 060619/883
libcurl					
Improper Restrictio n of Operatio ns 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/do cs/CVE- 2019- 5436.html	A-HAX-LIBC- 060619/884
heidelberg	3				
prinect_ar	chiver				
Improper Neutraliz ation of Input During Web Page Generatio n ('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	Pat	ch	NCIIP	CID
Horde							
groupware	e						
Improper Control of Generatio n 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.p hp, 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- 060619	
hybridgro							
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
gobot					
Improper Certificat e Validatio n	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_repor	ting_service				
Improper Neutraliz ation of Input During Web Page Generatio n ('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.	https://ww w.ibm.com/ support/do cview.wss? uid=ibm10 884604	A-IBM-JAZZ- 060619/888
cognos_an	alytics				
Improper Neutraliz ation of Input During Web Page Generatio n ('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
webspher	e_mq				

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	<b>8</b> -9	9-10
(CVSS)	0	1-2	7	†	7	3-0	0-7	7	5	J-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Informati on 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://ww w.ibm.com/ support/do cview.wss? uid=ibm10 870492	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.	https://ww w.ibm.com/ support/do cview.wss? uid=ibm10 872876	A-IBM-WEBS- 060619/891
api_connec	ct		CVE ID : CVE-2019-4078		
Inadequa te Encryptio n 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.	https://ww w.ibm.com/ support/do cview.wss? uid=ibm10 882968	A-IBM-API 060619/892
webspher	e_application_	server			
Deserializ ation of Untruste d 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://ww w.ibm.com/ support/do cview.wss? uid=ibm10 883628	A-IBM-WEBS- 060619/893
bigfix_plat	form				
CV Scoring (CVSS)	()-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutraliz ation of Input During Web Page Generatio n ('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.	https://ww w.ibm.com/ support/do cview.wss? uid=ibm10 881996	A-IBM-BIGF- 060619/894
J			CVE ID : CVE-2019-4011		
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://ww w.ibm.com/ support/do cview.wss? uid=ibm10 881996	A-IBM-BIGF- 060619/895
qradar_se	 curity_informa	tion_a	nd_event_manager		
Improper Certificat e Validatio n	WinCollect could alloattacker to obtain ser information by spoof trusted entity using middle techniques du validating or incorrect validating a certificat Force ID: 160072.		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-	https://ww w.ibm.com/ support/do cview.wss? uid=ibm10 885464	A-IBM-QRAD- 060619/896
cloud_priv	vate				
Improper Input Validatio n	oroper ut 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publis	h Date	CVSS	D	escription	ո & CVE II	D	Pat	tch	NCIIP	C ID
				158145.							
1				CVE ID :	CVE-20	19-411	9				
identityse	rver										
identityse	rver4										
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	21-05-	-2019	4.3	IdentityServer IdentityServer4 through 2.4 has stored XSS via the httpContext to the host/Extensions/RequestLogge rMiddleware.cs LogForErrorContext method, which can be triggered by viewing a log.  CVE ID: CVE-2019-12250				N/A		A-IDE-I 060619	
incsub											
hustle											
Improper Neutraliz ation of Special Elements in Output Used by a Downstre am Compone nt ('Injectio n')	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-H 060619	
Intel	<u> </u>										
acu_wizaro	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		
CV Scoring (CVSS)		0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	& CVE II	)	Pa	tch	NCIIP	CID
				authenti potentia privilege CVE ID:	lly enabl e via loca	le escala al access	•				
scs_discov	ery_uti	lity									
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-S 060619	
driver_&_s	upport	t_assista	ant					1			
Improper Access Control	17-05	-2019	2.1	Insufficient Intel(R) Assistant before muser to puse information access.  CVE ID:	Driver 8 t version nay allov potential tion disc	a Suppor 19.3.12 v a privi ly enabl losure v	rt 2.3 and leged e ia local	N/A		A-INT-I 060619	
Improper Input Validatio n	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-I 060619	
converged	_secur	ity_man	ageme	ent_engin	e_firmw	vare		_			
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-0 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unprivileged user to potentially enable escalation of privilege via local access.  CVE ID: CVE-2019-0086		
Improper Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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_ma	nagement_tech	nolog	у		
Improper Input Validatio n	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 Validatio n	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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish	Date	CVSS	D	Description & CVE ID					NCIIF	CID
				unauthe potentia service v access.	lly enab	le denia					
				CVE ID:	<b>CVE-20</b>	19-009	4				
Out-of- bounds Write	17-05-2	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.				N/A		A-INT-A 060619	
gwanhi aa d	luivou			CVE ID : CVE-2019-0096							
graphics_d	iriver			200			T				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2	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-0 060619		
Concurre nt Execution using Shared Resource with Improper Synchron ization ('Race Condition ')	17-05-2	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-0 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIP	C ID
Improper Input Validatio n	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-0 060619	
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-0 060619	-
unite							
Improper Input Validatio n	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-U 060619	
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-U 060619	
Jenkins							
CV Scoring		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch:	NCIIP	C ID
warnings_	next_generation	on								
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	31-05-2019	3.5	A cross- vulneral Warning earlier a Job/Con inject ar build ov CVE ID:	N/A		A-JEN-V 060619				
Cross- Site Request Forgery (CSRF)	31-05-2019	4.3	A cross-sulneral Warning earlier a reset wabuilds.	oility in J gs NG Plu llowed a rning co	enkins igin 5.0. ttackers unts for	0 and s to future	N/A		A-JEN-V 060619	
pluggable_	authenticatio	n_mod	ule							
N/A	21-05-2019	4	Jenkins I Plugin 1 1.4.1 in PamSecumpl#do' Overall/ obtain li about th the user	A missing permission check in Jenkins PAM Authentication Plugin 1.5 and earlier, except					A-JEN-F 060619	
credential	S									
File and Directory Informati on 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	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	Description & CVE ID			)	Pat	tch	NCIIP	CID
				obtain the files concertificat	taining a						
				CVE ID : CVE-2019-10320							
pipeline_n	maven_integration										
Improper Restrictio n of XML External Entity Referenc e ('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.			N/A		A-JEN-P 060619		
				CVE ID:	CVE-20	19-103	27				
pipeline_r	emote_	loader									
Protectio n Mechanis m Failure	31-05	-2019	6.5	Jenkins I Plugin 1 a custom security to invoke bypassin protection CVE ID:	.4 and eand whiteling that allowed arbitration arbitration.	arlier pr st for sc owed att ary meth il sandbo	ovided ript ackers lods, ox	N/A		A-JEN-P 060619	
Jfrog											
artifactory	7										
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.DescriptorI mpl#doTestConnection allowed users with				N/A		A-JFR-A 060619	
CV Scoring (CVSS)		0-1	1-2	<b>2-3</b> 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

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.DescriptorI mpl#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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pa	tch	NCIIP	CID
				ging, and UnifiedF Submit a schedule perform Gradle a promote builds, r							
Joomla											
Joomla!											
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	20-05	-2019	4.3	An issue Joomla! views of properly data, wh XSS atta CVE ID :	before 3 com_us escape ich lead ck vecto	.9.6. The ers do n user su s to a po r.	e debug ot pplied otential	N/A		A-J00-J 060619	
Jreast											
jr_east_jap	an										
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-J 060619	
karamaso	ft										
ultimateed	ditor										
Unrestric ted Upload of	24-05	-2019	7.5	Karamasoft UltimateEditor 1 does not ensure that an uploaded file is an image or						A-KAR- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	cvss	De	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
File with Dangerou s Type				nor exte The atta Attach io upload. A accessib Ultimate s/ URI.	ocument (neither file types or extensions are restricted). The attacker must use the stach icon to perform an oload. An uploaded file is reessible under the timateEditorInclude/UserFile URI.  VE ID: CVE-2019-12150						
Kentico					0.2 = 0						
kentico											
Improper Input Validatio n	22-05	-2019	6.4	Kentico attacker files with the cmsmod mcontro mageori URI.	s upload hout aut ules/me ils/livese nedia/ta	l and exp henticatedialibratelectors electors abs_med	olore ion via ary/for /inserti ia.aspx	N/A		A-KEN-1 060619	
Kibokolab	)S			CVE ID.	CVL 20	17 121					
hostel											
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	27-05	-2019	4.3	plugin b WordPr	exists in the Kiboko Hostel in before 1.1.4 for dPress. ID: CVE-2019-12345		N/A		A-KIB-H 060619		
leanify_pr	oject										
leanify											
Out-of- bounds	23-05	-2019	4.3	attacker	Leanify 0.4.3 allows remote attackers to trigger an out-of-bounds write (1024 bytes) via a		N/A		A-LEA-I 060619		
CV Scoring (CVSS		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			modified input file.		
			CVE ID : CVE-2019-12298		
Lemonlda	p-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 Derefere nce	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_s tate 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_imag	e				
Improper Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Derefere nce	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 Derefere nce	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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pat	tch	NCIIP	CID
				CVE ID :	CVE-20	19-122	20				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	estrictio of peratio s within ne ounds f a  Jemory  All Issue w libSDL2.a DirectMed when used 20-05-2019  4.3  Lemory  All Issue w libSDL2.i 2.0.4. Therefore the stdlib/SDI CVE ID : CVE ID : CVE ID : C					ayer (SDL) 2.0.9 conjunction with e.a in SDL2_image a SEGV in the DL_free_REAL at				A-LIB-S 060619	
simple_dir	ectmed	dia_laye	er								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	20-05-		4.3	libSDL2. DirectMonth when us libSDL2. 2.0.4. Th buffer of SDL2_im IMG_Loa	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					A-LIB-S 060619	
NULL Pointer Derefere nce	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-S 060619	
NULL Pointer Derefere nce	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	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6 6-7 7-8 8-9		8-9	9-10

Weakness	Publish Da	te CVSS	D	Description & CVE ID				ch	NCIIP	CID
			function IMG_pcx		adPCX_I	RW at				
			CVE ID:	<b>CVE-20</b>	19-122	18				
Double Free	20-05-201	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						A-LIB-S 060619		
Out-of- bounds Read	20-05-201	.9 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-S 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	20-05-201	.9 4.3	An issue libSDL2. DirectMowhen us libSDL2. 2.0.4. The SDL fund stdlib/S. CVE ID:	a in Simedia Layed in continuous and in continuo	ple er (SDL) njunctio in SDL2 SEGV in L_free_R oc.c.	2.0.9 n with _image the EAL at	N/A		A-LIB-S 060619	
Out-of- bounds Read	20-05-201	.9 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-S 060619	
CV Scoring (CVSS)		-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h NCIIPC ID
			video/SDL_pixels.c.		
			CVE ID : CVE-2019-12222		
macdown_	project				
macdown					
Improper Limitatio n of a Pathnam e to a Restricte d 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 Validatio n	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.	N/A	A-MAC- MACD- 060619/948
			CVE ID : CVE-2019-12173		
matomo					
matomo					
Informati on 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 discover lastError. File is used a plugins/CorePluginsAdmin/tomplates/safemode.twig. NOT the vendor disputes the significance of this issue, stating "avoid reporting path disclosures, as we don't	sk, n N/A	A-MAT- MATO- 060619/949
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publis	h Date	CVSS	De	Description & CVE ID			Pat	tch	NCIIP	C ID
				consider vulneral		s securit	у				
						10 122	<b>1</b> F				
241				CVE ID : CVE-2019-12215							
Microsoft											
nuget								1			
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-N 060619	
visual_stu	dio										
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-\ 060619	
chakracor	e										
Improper Restrictio n of Operatio ns 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-( 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	3-4 4-5 5-6		6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory			Vulnerability'. This CVE ID is unique from CVE-2019-0884, CVE-2019-0918.		
Buffer			CVE ID : CVE-2019-0911		
Improper Restrictio n of Operatio ns 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-2019-0927, CVE-2019-0923, CVE-2019-0923, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937.  CVE ID: CVE-2019-0912	N/A	A-MIC-CHAK- 060619/953
Improper Restrictio n of Operatio ns 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-2019-0927, CVE-2019-0923, CVE-2019-0923, CVE-2019-0923, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937.	N/A	A-MIC-CHAK- 060619/954
Improper	16-05-2019	7.6	A remote code execution	N/A	A-MIC-CHAK-
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID	
Restriction of operations within the Bounds of a Memory Buffer				vulneral that the engine h memory 'Chakra Memory Vulnera unique f CVE-202 0915, CV 2019-09 CVE-202 0924, CV 2019-09			060619	/955				
				CVE ID :								
Improper Restrictio n of Operatio ns 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-2019-0927, CVE-2019-0923, CVE-2019-0923, CVE-2019-0923, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937.				N/A		A-MIC-0 060619		
Improper Restrictio n of Operatio ns 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		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	3-4 4-5 5-6			7-8	8-9	9-10	

Weakness	Publish	Date	cvss	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
of a Memory Buffer				Vulnera unique f CVE-202 0914, CV 2019-09 CVE-202 0924, CV 2019-09 CVE-202							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2	2019	7.6	Memory Vulnera unique f CVE-202 0914, CV 2019-09 CVE-202 0924, CV 2019-09 CVE-202	bility exichality exicandles of in Microscopius of the Corruption	sts in the scripting objects in the control of the	e way g g ge, aka e ID is 0912, 119- EVE- 922, 119- EVE- 933,	N/A		A-MIC-0 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2	2019	7.6	CVE-2019-0937.  CVE ID: CVE-2019-0917  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-0 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Restrictio n of Operatio ns 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-2019-0925, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937.  CVE ID: CVE-2019-0924	N/A	A-MIC-CHAK- 060619/960
Improper Restrictio n of Operatio ns 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-
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-	-8 8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIPC ID
Restrictio n of Operatio ns 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-2019-0926, CVE-2019-0927, CVE-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0933, CVE-2019-0937.			060619/962
Improper Restrictio n of Operatio ns 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-2019-0922, CVE-2019-0923, CVE-2019-0924, CVE-2019-0925, CVE-2019-0927, CVE-2019-0937.	N/A		A-MIC-CHAK- 060619/963
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	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.			
edge						
Improper Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pat	tch	NCIIP	CID
Memory Buffer			CVE-201 0915, CV 2019-09 CVE-201 0924, CV 2019-09 CVE-201	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.						
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	7.6	A remotivulneral that the engine has memory 'Chakra Memory Vulneral unique for CVE-2019-09	bility exicandles of in Micros Scripting Corruption CVI 19-0914 VE-2019 VE-201	sts in the scripting objects in the control of the	e way g g n ge, aka e ID is 0912, 119- EVE- 922, 119- EVE- 933,	N/A		A-MIC-I 060619	
Improper Restrictio n of Operatio ns 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-I 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Dat	e CVSS	D	Description & CVE ID				tch	NCIIP	C ID
			2019-09 CVE-201	•		933,				
			CVE ID :	CVE-20	19-091	4				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	7.6	vulneral that the engine h memory 'Chakra Memory Vulneral unique f CVE-201 0914, CV 2019-09 CVE-201 0924, CV 2019-09 CVE-201	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-2019-0927, CVE-2019-0923, CVE-2019-0923, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937.  CVE ID: CVE-2019-0915					A-MIC-E 060619	
Improper Restrictio n of Operatio ns 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-2019-0917, CVE-2019-0922, CVE-2019-0923, CVE-2019-0923, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937.  CVE ID: CVE-2019-0916			N/A		A-MIC-E 060619		
Improper Restrictio	16-05-2019	7.6	A remote code execution vulnerability exists in the way			N/A		A-MIC-E 060619		
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	cvss	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
n of Operatio ns 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-2019-0924, CVE-2019-0923, CVE-2019-0923, CVE-2019-0927, CVE-2019-0927, CVE-2019-0933, CVE-2019-0937.							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05	-2019	7.6	vulneral that the engine h memory 'Chakra Memory Vulneral unique f CVE-202 0914, CV 2019-09 CVE-202 0924, CV 2019-09	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-2019-0923, CVE-2019-0923, CVE-2019-0927, CVE-2019-0923, CVE-2019-0933, CVE-2019-0937.					A-MIC-I 060619	
Improper Restrictio n of Operatio ns 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-I 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	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.				
Improper Restrictio n of Operatio ns 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-EDG 060619/97	
Improper Restrictio n of Operatio ns 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-	N/A		A-MIC-EDG 060619/97	
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-	-10

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	CID
			2019-09 CVE-201 CVE ID :	9-0937.		·				
Improper Restrictio n of Operatio ns 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-I 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	7.6	A remotivulneral that the engine himemory 'Chakra Memory Vulneral unique ff CVE-201 0914, CVE-201 0923, CVE-201 CVE-201 CVE-201 CVE-201	chakra s chakra s andles o in Micro Scripting Corrupt bility'. The 9-0913, 7E-2019- 9-0922, 7E-2019- 25, CVE- 9-0937.	sts in the scripting objects in the scripting objects in the scripting Engine cion of the scripting of the s	e way g g ge, aka e ID is 19- 19- 19- 19- 19- 19- 19- 19- 19- 19-	N/A		A-MIC-I 060619	
Improper Restrictio n of Operatio ns 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-I 060619		
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			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 Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			CVE ID : CVE-2019-0940		
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.	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	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			0946.							
			CVE ID :	CVE-20	19-094	7				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote vulneral Word so properly memory Remote Vulneral CVE ID:	oility exist ftware we handle f, aka 'Mi Code Exection	sts in Mi when it fobjects crosoft ecution	icrosoft ails to in Word	N/A		A-MIC-0 060619	
office_365	_proplus	1					L			
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-0 060619	
Improper Restrictio n of Operatio ns 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-0 060619		
internet_e	xplorer									
Improper Restrictio n of	16-05-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles			e way	N/A		A-MIC-I 060619	
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pate	ch	NCIIPC ID
Operatio ns within the Bounds of a Memory			objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0911, CVE-2019-0918.			
Buffer			CVE ID : CVE-2019-0884			
Improper Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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 Validatio n	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 Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Bounds			Corruption Vulnerability'.		
of a Memory Buffer			CVE ID : CVE-2019-0929		
Informati on 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 Restrictio n of Operatio ns 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 Validatio n	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-MICNET- 060619/997
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7	7-8 8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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.	N/A	A-MICNET- 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-MICNET- 060619/999
.net_frame	ework				
Improper Input Validatio n	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-MICNET- 060619/1000
Improper Restrictio n of Operatio ns 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-MICNET- 060619/1001
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7	-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	ch	NCIIP	CID
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-MICN 060619,	
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-MICN 060619,	
visual_stuc	dio_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-V 060619,	
CV Scoring	Scale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	escription	& CVE II	)	Pat	ch	NCIIP	C ID
asp.net_co	re									
N/A	16-05-2019	5	A denial exists when the control of	hen ASP. erly hand s, aka 'AS f Service	NET Co lles web P.NET ( Vulnera	re Core ability'.	N/A		A-MIC- <i>A</i> 060619	
sharepoin	t_server						l			
Improper Input Validatio n	16-05-2019	3.5	A spoofi when Mi Server d sanitize request SharePo 'Microso Vulneral unique f CVE-201	icrosoft Soes not paspecial to an affect of the Share foility'. The community of the CVE	SharePo properly ly crafte ected er, aka Point Sp nis CVE	int 7 ed web 900fing ID is 9950,	N/A		A-MIC-S 060619	
Improper Input Validatio n	16-05-2019	3.5	A spoofi when Mi Server d sanitize request SharePo 'Microso Vulneral unique f CVE-201	icrosoft soes not paspecial to an affect of the Share foility'. The community of the commun	SharePo properly ly crafte ected er, aka Point Sp nis CVE	int ded web ooofing ID is	N/A		A-MIC-S 060619	
N/A	16-05-2019	6.5	An eleva vulneral Microso does not specially an affect aka 'Mic Elevatio Vulneral	pility exists of the Share For the Control of Private	sts when Point Sen y sanitiz web rec Point so narePoir ilege	rver ze a quest to erver,	N/A		A-MIC-S 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				unique f	rom CVE	E-2019-0	958.				
				CVE ID:	CVE-20	19-095	7				
N/A	16-05	-2019	6.5	An eleval vulneral Microso does not specially an affect aka 'Mic Elevatio Vulneral unique f	pility exists of Share It is properly crafted share rosoft Share of Priville in CVE	sts where of the control of the cont	ever ase a quest to erver, at D is 1957.	N/A		A-MIC-S 060619	
word											
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-	-2019	9.3	A remote vulneral Word so properly memory Remote Vulneral CVE ID:	oility exist oftware v handle r, aka 'Mi Code Exe bility'.	sts in Mi when it f objects : crosoft ' ecution	crosoft ails to in Word	N/A		A-MIC-\ 060619	
sharepoin	t_enter	prise_s	erver								
N/A	16-05-	-2019	6	A remotivulneral SharePoto propeunsafe Aaka 'Mic Server R' Vulneral CVE ID:	oility eximint Serve int Serve erly ident SP.Net v rosoft Sh demote C bility'.	sts in Mi er when tify and veb cont narePoir ode Exe	crosoft it fails filter rols, it cution	N/A		A-MIC-S 060619	
- 0				An infor							
Informati on Exposure	16-05-	-2019	4	vulneral Microso does not	oility exi ft ShareI	sts wher Point Ser	n ver	N/A		A-MIC-S 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
				specially an affect aka 'Mic Server In Vulneral	ed Share rosoft Sl nformati bility'.	ePoint sonarePoin	erver, nt losure				
N/A	16-05-		6.5	An eleval vulneral Microso does not specially an affect aka 'Mic Elevatio Vulneral unique f	pility exi ft Sharel t properl crafted red Share rosoft Sh n of Priv bility'. The	sts when Point Sendy sanitize web rece Point senarePoint rilege his CVE E-2019-0	n rver ze a quest to erver, nt ID is 0958.	N/A		A-MIC-S 060619	
office_onli	ne_serv	/er									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-	-2019	9.3	A remotivulneral Word so properly memory Remote Vulneral CVE ID:	oility exi oftware v handle r, aka 'Mi Code Ex bility'.	sts in M when it f objects icrosoft ecution	icrosoft Tails to in Word	N/A		A-MIC-0 060619	
sharepoin	t_found	lation									
Improper Input Validatio n	16-05-	-2019	3.5	A spoofi when Mi Server d sanitize request SharePo 'Microso Vulneral unique f CVE-201	icrosoft oes not a special to an affint serve oft Share bility'. The common CVI	SharePo properly lly crafto ected er, aka Point Sp his CVE	oint  V  ed web  coofing  ID is	N/A		A-MIC-S 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publisl	h Date	cvss	D	escriptio	n & CVE II	D	Pat	tch	NCIIP	CID
				CVE ID :	CVE-20	19-094	.9				
Improper Input Validatio n	16-05-	2019	3.5	A spoofi when M Server d sanitize request SharePo 'Microso Vulnera unique f CVE-202	icrosoft loes not a specia to an aff int serve oft Share bility'. T	SharePo properly lly crafto ected er, aka Point Sp his CVE E-2019-0	N/A		A-MIC-9 060619		
				CVE ID :	CVE-20	19-095	0				
Improper Input Validatio n	16-05-	2019	3.5	A spoofi when M Server d sanitize request SharePo 'Microso Vulnera unique f CVE-202	icrosoft loes not a specia to an aff oint serve oft Share bility'. T Grom CVI	SharePo properly lly crafto ected er, aka Point Sp his CVE E-2019-0	oint y ed web ooofing ID is 0949,	N/A		A-MIC-9 060619	
N/A	16-05-	2019	6	A remotivulneral SharePoto properunsafe A aka 'Mic Server F Vulnera	e code e bility exi bint Serv erly iden ASP.Net v rosoft Si Remote ( bility'.	xecution sts in M er when tify and web cont harePoin Code Exe	icrosoft it fails filter trols, it	N/A		A-MIC-9 060619	
Informati on Exposure	16-05-	2019	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			erability exists when cosoft SharePoint Server snot properly sanitize a cially crafted web request to ffected SharePoint server,				A-MIC-S 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server 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 Neutraliz ation of Input During Web Page Generatio n ('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				1	
Informati on 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_foun	dation_server				
Improper Neutraliz ation 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
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	cvss	De	escription	a & CVE II	)	Pa	tch	NCIIP	C ID
Web Page Generatio n ('Cross- site Scripting' )				input, ale Server a Server C Vulneral unique f	nd Team ross-site bility'. Tl rom CVE	Founda Scripti his CVE E-2019-0	ation ng ID is )979.				
Informati on Exposure	16-05	-2019	9	An inforvulneral DevOps Team For properly crafted a to an affination and the control of the cont	oility exi Server a bundation sanitized authention ected serviced services bevops Soundation bility'.	sts when nd Micr n Serven e a speci cation re rver, aka erver ar n Serven	n Azure osoft do not ally equest a	N/A		A-MIC-7 060619	
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	16-05	-2019	3.5	A Cross-vulneral DevOps Foundat properly input, als Server a Server Coulneral unique for the CVE ID:	oility exicion Server a sanitized to a 'Azure and Team cross-site bility'. The come CVE	sts when nd Team er do no e user pr e DevOpe n Founda e Scripti his CVE E-2019-0	n Azure n ot rovided s ation ng ID is 0872.	N/A		A-MIC-7 060619	
visual_stu	dio_202	19	I								
N/A	16-05	-2019	7.2	An eleval vulneral Diagnos Collector Standard deletion location vulneral first hav	pility exitics Hub r or the V d Collect in arbiti s.To exp	sts when Standar Visual St or allow rary loit the attacker	n the rd cudio rs file r would	N/A		A-MIC-\ 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	n & CVE II	D	Pat	tch	NCIIP	CID
				system, a Standard Studio S Elevatio Vulneral	d Collect tandard n of Priv	cor, Visu Collecto	al				
	l			CVE ID :	CVE-20	19-072	7				
sql_server											
Informati on Exposure	16-05	-2019	4	An inforvulnerate SQL Services Disclosu	oility exiver Analy imprope a permisoft SQL S Informa re Vulne	sts in Managerly enfo erly enfo erssions, a erver Anation erability	icrosoft vices rces ka nalysis	N/A		A-MIC-S 060619	_
office_365											
N/A	16-05	-2019	9.3	A remote vulneral Microsoft Connect handles 'Microsoft Connect Code Exert This CVE CVE-2010947.	oility exift Office ivity English Office ivity English ElD is un	sts when Access gine imp in memo Access gine Ren Vulneral nique fro , CVE-20	n the properly pry, aka note bility'. om 119-	N/A		A-MIC-0 060619	
azure_acti	ve_dire	ectory_c	onnect	ţ							
N/A	16-05	-2019	3.5	An eleva vulnerate Azure Ad build 1.3 attacker PowerSh of a priv perform	oility exictive Dir 3.20.0, w to execu nell cmd ileged a	sts in Marectory ( Thich alloute two lets in co	icrosoft Connect ows an ontext	N/A		A-MIC- <i>I</i> 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	& CVE II	D	Pat	tch	NCIIP	C ID
				exploit to need to a AzureÂ? aka 'Mic Connect Vulneral CVE ID:	authenti AD Con rosoft Az Elevatio pility'.	cate to t nect ser zure AD on of Pri	he ver, vilege				
dynamics_	365							•			
N/A	16-05-	-2019	4.3	A securi vulneral Dynamic 'Microso Premise Bypass'.	oility exists on Present of the Dynar Security	sts in emise, al mics On- Feature	ka - e	N/A		A-MIC-I 060619	
dynamics_	crm_20	)15									
N/A	16-05-	-2019	4.3	A securi vulneral Dynamic 'Microso Premise Bypass'.	oility exists on Present of the Dynar Security	sts in emise, al mics On- Feature	ka - e	N/A		A-MIC-I 060619	
Mylittlefor	rum										
my_little_f	orum										
Cross- Site Request Forgery (CSRF)	21-05-	-2019	5.8	my little allows C demons mode=p <b>CVE ID</b> :	SRF to d trated by osting&o	elete po <sup>7</sup> delete_p	osts, as	N/A		A-MYL- 060619	_
Nagios											
nagios_xi											
Improper Neutraliz ation of Special Elements	22-05-	-2019	7.5	Nagios X injectior paramet login.ph	via the er to	usernan	ne	N/A		A-NAG- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	cvss	D	escriptio	n & CVE II	D	Pa	tch	NCIIF	PC ID
used in				reset pa	ssword	form).					
an SQL				CVE ID :	CVE-20	19-122	79				
Comman											
d ('SQL											
Injection'											
)											
Netgate											
Pfsense											
Improper Access Control	20-05	-2019	6.5	Incorrect WebUI i version before 2 authenti privilege a specia	n OPNse 19.1.8, a .4.4-p3 icated uses to adr lly crafte	ense befo and pfser allows ro sers to e ministrated ed reque	ore nse emote scalate tor via	https://w.netgom/bl/sense-4-relep3-noavailaml	gate.c og/pf 2-4- ase- w-	A-NET- 060619	
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	29-05	-2019	4.3	In pfSen XSS vulr attacker the Nam via an acme_ac action. T due to in	nerability s inject e or Des countke he vuln nput vali	y occurs a payloa scription eys_edit.j erability	when d into a field php coccurs errors.	N/A		A-NET- 060619	
Nginx											
njs											
Improper Restrictio n of Operatio ns within the Bounds of a Memory	20-05	-2019	7.5	njs throm NGINX, l overflow nxt_utf8	has a heav v in nxt_ .c.	ap-based utf8_end	d buffer code in	N/A		A-NGI-1 060619	•
	<u> </u>									<u> </u>	
CV Scoring		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer					
Improper Restrictio n of Operatio ns 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 Restrictio n of Operatio ns 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					
-	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
Improper Neutraliz ation of Special Elements used in a Comman d ('Comma	23-05-2019	7.5	the endpoints admin/status/realtime/bandwi dth_status and admin/status/realtime/wireles s_status of the web application are affected by a command injection vulnerability.	N/A	
luci Improper Neutraliz ation of Special Elements used in a Comman d ('Comma nd Injection' ) Oracle enterprise	23-05-2019 e_manager_ops		the endpoints admin/status/realtime/bandwi dth_status and admin/status/realtime/wireles s_status of the web application are affected by a command injection vulnerability.  CVE ID: CVE-2019-12272	N/A	
Iuci Improper Neutraliz ation of Special Elements used in a Comman d ('Comma nd Injection' ) Oracle			the endpoints admin/status/realtime/bandwi dth_status and admin/status/realtime/wireles s_status of the web application are affected by a command injection vulnerability.  CVE ID: CVE-2019-12272	N/A	

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 Neutraliz ation of Input During Web Page Generatio n ('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://co mmunity.ot rs.com/secu rity- advisory- 2019-06- security- update-for- otrs- framework /	A-OTR-OTRS- 060619/1041
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Web Page   21-05-2019   3.5   Who is logged into 01 K5 as all   2019-05-	R-OTRS- 9/1042
CVE ID : CVE-2019-10066	
Improper Neutraliz ation of Input During Web Page Generatio n ('Crosssite Scripting' )  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  An issue was discovered in Open Ticket Request System (OTRS) 7.x through 7.0.6 and rity-raciomy. A-OTR 2019-05-security-update-for-otrs-framework framework //	
Improper Neutraliz ation of Input During Web Page Generatio n ('Crosssite Scripting' )  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.ot rs.com/secu rity-advisory-2019-05-security-update-for-otrs-framework /	
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	8-OTRS- 9/1043
Ovirt	
cockpit-ovirt	
N/A   17-05-2019   2.1   engine   '   -	-COCK- 9/1044
CV Scoring Scale (CVSS)         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			of the deployment procedure, these files are deleted.  CVE ID: CVE-2019-10139		
Pandasecu	irity				
panda_gol	d_protection				
N/A	23-05-2019	10	Insecure permissions of the section object Global\PandaDevicesAgentShar edMemory and the event Global\PandaDevicesAgentShar edMemoryChange 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://ww w.pandasec urity.com/u sa/support /card?id=1 00063	A-PAN-PAND- 060619/1045
Percona					
percona_s	erver				
Improper Authentic ation	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					

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publis	h Date	CVSS	D	escription	a & CVE II	D	Pat	tch	NCIIP	CID
Improper Access Control	20-05	-2019	6.5	Incorrect WebUI in version before 2 authenti privilege a special	n OPNse 19.1.8, a .4.4-p3 a cated us es to adn lly crafte	nse beford pfser allows reserved to end to e	ore use emote scalate tor via est.	https:/ w.netg om/bl sense- 4-rele p3-no availal ml	gate.c og/pf ·2-4- ase- w-	A-PFS-F 060619	
Phome											
empirecm	s										
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	27-05	-2019	4.3	Empire( the from e/memb demonst payload dynamic attacker the e/templ hp regist page.  CVE ID:	parame per/doad trated by that cha c page te can cho ate/men tered acc	eter to etion.php y a CSRF nges the mplate. ose to re nber/re tivation	p, as e The esend gsend.p mail	N/A		A-PHO- 060619	
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	27-05	-2019	4.3	Empire() the HTT e/memb	P Refere er/doac	r heade tion.php	r to o.	N/A		A-PHO- 060619	
phprelativ	epath_	project									
phprelativ	epath										
Improper Neutraliz ation of	31-05	-2019	4.3	An XSS v PHPRela Path) th	ıtivePatl	ı (aka Ro	elative	N/A		A-PHP-1 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generatio n ('Crosssite Scripting' )			RelativePath.Example1.php path parameter.  CVE ID: CVE-2019-12507		
Prestasho	p				
prestasho	p				
Improper Neutraliz ation of Input During Web Page Generatio n ('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 Derefere nce	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 Wraparo und	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	Pat	ch	NCIIP	C 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-I 060619	
Revive-ad:	server						
revive_ads	server						
Use of Cryptogr aphically Weak Pseudo- Random Number Generato r (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-I 060619	
Sensiolabs	5	I.					
symfony							
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutraliz ation of Input During Web Page Generatio n ('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 Neutraliz ation of Special Elements used in an SQL Comman d ('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://sym fony.com/bl og/cve- 2019- 10910- check- service-ids- are-valid	A-SEN-SYMF- 060619/1057
Improper Authentic ation	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://sym fony.com/bl og/cve- 2019- 10911-add- a- separator- in-the- remember- me-cookie- hash	A-SEN-SYMF- 060619/1058
Deserializ ation of Untruste d 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://sym fony.com/bl og/cve- 2019- 10912- prevent-	A-SEN-SYMF- 060619/1059
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	cvss	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID	
				of files the access to symfony symfony	hat the control that th	current u related and it-bridge	iser has to e.	destru -with- effects from-l unseri	side- ;- peing-			
				CVE ID :								
Improper Neutraliz ation of Special Elements used in an SQL Comman d ('SQL Injection' )	16-05	-2019	7.5	In Symford before 2 4.x before 4 provided overrided as trusted not valid SQL inject related to the foundation of the symbol symb	.8.50, 3 re 4.1.12 .2.7, HT d as verb e header ed input, lated, po ction or co symfo	x before 2, and 4.2 IP Meth os or usi may be but the ossibly co XSS. Thi ny/http	3.4.26, 2.x ods ng the treated y are ausing is is	https:/ fony.co og/cve 2019- 10913 reject- invalid http- metho overri	om/bl e- d- d-	A-SEN-S 060619		
simmly hoo	1.			CVE ID :	CVE-ZU	119-109	13					
simplyboo simplyboo												
Unrestric	· K							l				
ted Upload of File with Dangerou s Type	17-05	-2019	7.5	SimplyB 05-11 do restrict l allow re CVE ID:	oes not p File Uplo mote co	oroperly oad whic de execu	ch could	https://ne ws.simplyb ook.me/not ification/		A-SIM-S 060619		
Soumu												
electronic	recept	tion_and	l_exam	nination_	of_appli	ication_	for_radi	o_licen	ses			
Untruste d Search Path	17-05	-2019	6.8	Untrusted vulneral Electron examinal radio lice and earl to gain pulnerse Didirectory CVE ID:	oility in laic reception of a enses Orier alloworivilege LL in an y.	Installer tion and applicati nline 1.0 vs an att s via a T unspeci	on for 1.9.0 acker rojan fied	N/A		N/A A-SOU- 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publis	h Date	CVSS	D	escription	n & CVE I	D	Pat	tch	NCIIP	CID
Untruste d Search Path	17-05-	-2019	6.8	vulneral receptio applicat Offline 1 allows a privilege DLL in a	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-1 060619	
Sqlite											
sqlite											
Out-of- bounds Read	30-05-	-2019	7.5	SQLite3 including to heap the rtree handling	g 3.27.2 out-of-b enode() g invalid	is vulne ound re function rtree ta	rable ad in when bles.	N/A		A-SQL-S 060619	•
synacor											
zimbra_co	llabora	tion_su	ite								
Deserializ ation of Untruste d Data	29-05-	-2019	7.5	Synacor Suite 8.7 allows in deserial compon	.x throunsecure ization is ent.	gh 8.8.1 object n the IM	1 AP	N/A		A-SYN-2 060619	
Server- Side Request Forgery (SSRF)	29-05-	-2019	4	Zimbra ( 8.7.x thr Blind SS compon	Collabor ough 8.8 RF in the ent.	ation Su 3.11 allo e Feed	uite ws	N/A		A-SYN-ZIMB- 060619/1066	
Improper Restrictio n of XML External Entity Referenc e ('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-2 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	cvss	D	escription	n & CVE I	D	Pa	tch	NCIIF	PC ID
tinycc											
tinycc											
Out-of- bounds Write	31-05	-2019	4.3	An issue C Compi 0.9.27. C source f out-of-b gsym_ac gen.c. Th tccasm.c switches	ller (aka Compilin ile leads ounds w ldr funct nis occur mishan	TinyCC g a craft to a one rite in t tion in x rs becau dles sec	or TCC) ted e-byte he 86_64- se tion	N/A		A-TIN-7 060619	
Torproject	t										
tor_brows	er										
Informati on Exposure	27-05	-2019	4.3	Tor Brown an informattacker browser measuring the usunguage	mation edility. It as to detection of the control o	exposure allows r ect the ale by ton wid "Don't s g.	emote th, even end my	N/A		A-TOR- 060619	_
typora											
typora											
Improper Limitatio n of a Pathnam e to a Restricte d 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-' 060619		
Improper Input	17-05	-2019	6.8		0.9.9.21.1 (1913) arbitrary code execution			N/A		A-TYP-	ГҮРО-
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validatio n			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_proj	ect				
ucms					
Improper Neutraliz ation of Special Elements used in an SQL Comman d ('SQL Injection' )	21-05-2019	6.5	sadmin/ceditpost.php in UCMS 1.4.7 allows SQL Injection via the index.php?do=sadmin_ceditpos t cvalue parameter.  CVE ID: CVE-2019-12251	N/A	A-UCM-UCMS- 060619/1072
virim_proj	ject				
virim					
Deserializ ation of Untruste d 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	1				
Improper Neutraliz ation 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Comman d ('SQL Injection' )					
webpaget	est				
webpaget	est				
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 Neutraliz ation of Input During Web Page Generatio n ('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 Neutraliz ation of Input During Web Page Generatio n ('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
	Scale			_	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Wireshark	<b>K</b>				
wireshark					
Improper Control of Generatio n 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		A-WIR-WIRE- 060619/1078
Wolfssl					
wolfssl					
Improper Restrictio n of Operatio ns 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

CV Scoring Scale	0-1	1_2	2-3	2-1	<b>1</b> -5	5-6	6-7	7₋0	8-9	0_10
(CVSS)	0-1	1-2	2-3	3-4	4-5	3-0	0-7	7-0	0-9	3-10

Weakness	Publis	h Date	cvss	D	escription	n & CVE I	D	Pat	tch	NCIIP	C ID
Wpbookin	gsyste	m									
wp_bookir	ıg_syst	em									
Improper Neutraliz ation of Special Elements used in an SQL Comman d ('SQL Injection' )	20-05	-2019	6.5	The WP 1.5.1 for CSRF pr attacker injection adminis CVE ID:	ress has , which ch certai that req ccess.	no allows n SQL uire	N/A		A-WPB- WP_B- 060619		
Wso2	Wso2										
api_manag	ger										
Unrestric ted Upload of File with Dangerou s Type	21-05	-2019	5.5	WSO2 A possible upload, any type extension	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					A-WSO- 060619	_
Zohocorp											
manageen	gine_se	erviced	esk_plu	ıs							
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	21-05		4.3	An issue Zoho Ma ServiceI XSS via tield.  CVE ID:	nnageEn Desk Plu The Sear CVE-20	gine s 9.3. Th chN.do s <b>119-121</b> Engine	ere is search	N/A		A-ZOH- MANA- 060619/1082	
N/A	21-05	-2019	4	ServiceDesk Plus through 10.5, users with the lowest privileges			N/A		MANA- 060619	/1083	
_	CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6				5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch:	NCIIP	C ID
			(guest) of post by a to the SDNotify ution&n Mail&no & & & & & & & & & & & & & & & & & &	appending.do?not node=E- otifyTo=Sostring.	ng its nu ifyModu SOLFOR'	mber le=Sol WARD				
manageen	gine_adselfse	rvice_p	lus							
Improper Neutraliz ation of Input During Web Page Generatio n ('Crosssite Scripting' )	24-05-2019	4.3	In Zoho ADSelfSo 5704, ar cross-sit vulneral unauthe of the Ja injecting paramet can use AD self-s and MFA CVE ID:	ervice Planauthorice Scription in the Scription of the HT ser adscstation to case which the the the the the the the the the th	us 5.x the zation.d ing (XSS ows for a manipul code by Form of an attention asswore a sasswore a sa	o ) an llation tacker user's	N/A		A-ZOH- MANA- 060619	/1084
manageen	gine_netflow_	analyz	er							
Improper Limitatio n of a Pathnam e to a Restricte d 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/CReportPDFS ervlet (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
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutraliz ation of Input During Web Page Generatio n ('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 Neutraliz ation of Input During Web Page Generatio n ('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 Neutraliz ation of Input During Web Page Generatio n ('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/userManageme ntForm.jsp via these GET parameters: authMeth, passWord, pwd1, and userName.  CVE ID: CVE-2019-8928	N/A	A-ZOH- MANA- 060619/1088
Improper Neutraliz ation 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

		VCC oviete in the Administration				
		zone /netflow/jspui/selectDevice.jsp file in these GET parameters: param and rtype.  CVE ID : CVE-2019-8929  Operating System	etflow/jspui/selectDevice.jsp in these GET parameters: am and rtype. E ID : CVE-2019-8929			
sy_controller_f	irmwa	re				
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.	https://me dia.boschse curity.com/ fs/media/p b/security_ advisories/ bosch- 2019- 0403bt-cve- 2019- 6957_securi ty_advisory _software_b uffer_overfl ow.pdf	O-BOS-ACCE- 060619/1090		
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://me dia.boschse curity.com/ fs/media/p b/security_ advisories/ bosch- 2019-	0-B0S-ACCE- 060619/1091		
	29-05-2019	29-05-2019 7.5	Operating System  Sy_controller_firmware  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  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	Operating System  Sy_controller_firmware  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  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 2019-  Operating System  https://me dia.boschse curity-advisories/bosch-2019-  https://me dia.boschse-curity-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 2019-		

Weakness	Publis	h Date	CVSS	Description & CVE ID			Pat	tch	NCIIP	CID	
				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			0404b 2019- 6958_ ty_adv _impro access rol.pd:	securi risory oper_ _cont			
dip_3000_1	firmwa	ire									
Improper Restrictio n of Operatio ns 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:/dia.bo curity.fs/med b/sect advisor bosch- 2019- 0403b 2019- ty_adv _softw uffer_o	schse .com/ dia/p .rityries/ ot-cve- securi risory .rare_b .overfl	0-B0S-1 060619	_	
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,			dia.boschse curity.com/		0-B0S-1 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5 5-6 6-7 7-8			8-9	9-10	

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch:	NCIIP	C 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/secu adviso bosch- 2019- 0404b 2019- 6958_t ty_adv _impro access rol.pdf	ries/ t-cve- securi isory oper_ _cont		
dip_7000_1	firmware									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	29-05-2019	7.5	vulneral Video M (BVMS) DIVAR II 7000, Vi Manager Streamin Configur Building (BIS) wi Professi Access E Bosch V Video SI vulneral the unau code in t network	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				//me schse com/ dia/p irity_ ries/ t-cve- securi isory are_b overfl f	0-B0S-1 060619	_
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	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://me dia.boschse curity.com/ fs/media/p b/security_ advisories/ bosch- 2019- 0404bt-cve- 2019- 6958_securi ty_advisory _improper_ access_cont rol.pdf	O-BOS-DIP 060619/1095
Cisco					
nx-os					
Improper Neutraliz ation of Special Elements used in a Comman d ('Comma nd 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	tch	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_de	elivery <sub>.</sub>	_controller_firmware				
Improper Restrictio n of Operatio ns 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		0-CIT-NETS 060619/109	
netscaler_	gateway_firmv	vare					
Improper Restrictio n of Operatio ns 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		0-CIT-NETS 060619/109	
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 <b>9-</b> 1	10

Weakness	Publish	Date	cvss	De	escription	& CVE II	)	Pa	tch	NCIIP	CID
				12.1.49.	23.						
				CVE ID:	CVE-20	19-120	44				
Debian											
debian_lin	ux										
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:/keepe he.org rity.ht VE-20 0201	r.apac /secu ml#C	O-DEB- 060619	
Improper Access Control	22-05-2	2019	7.5	LemonL Incorrect CVE ID :	t Access	Control		N/A		O-DEB- 060619	
Informati on Exposure	17-05-2	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- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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.MiniA dmin 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

4-5

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish	h Date	CVSS	D	escription	a & CVE II	D	Pat	tch	NCIIP	C ID
				Report S result in files on t	reading	of arbit	trary				
				CVE ID:	CVE-20	19-989	2				
Emerson											
liebert_cha	allenge	r_firmv	vare								
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	22-05-	2019	4.3	httpGetS Emerson Liebert ( devices s statusstr	n Netwo Challeng allows X r parame	rk Powe er 5.1E( SS via th eter.	er ).5 1e	N/A		O-EME- 060619	
ovation_o	:r400_fi	irmwar	e								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	28-05-	2019	6.5	Controll heap-ba vulneral third-pa imprope commar which morruptic controlle code execution of privile.	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.					O-EME- 060619	
Improper Restrictio n of Operatio ns 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- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publisl	h Date	CVSS	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
Memory Buffer				cause the buffers, execution privilego	leading on and es	to remo	te code				
				CVE ID :	CVE-20	19-109	67				
Fedorapro	ject										
fedora											
N/A	22-05-	2019	6.5	A vulner libvirt > admin.se admin.se missing configur any user using virtlogd perform against to virtlogd CVE ID:	= 4.1.0 in ocket an ocket synthem ocket. Socket Martion particular on the land of the wirtle daemon	n the vir d virtlog stemd u lode arameter host to condition of the sock and strative ockd and strative as.	tlockd- gd- nits. A c allows connect ock or d tasks	N/A		O-FED-1 060619	
N/A	24-05-	2019	6.9	It was did to and in does not logrotat attacker control descalate by tricking to a direction inaccess user.	ncluding t correct e, allowi who alr of the ra his priv ng logro a radius ectory no	version ly config ng a loca eady ha diusd us ileges to otate into d-writal ormally he radiu	3.0.19 gure al s ser to root, o ole file	https:/ ub.cor eRADI eeradi server /2666	n/Fre US/fr us- r/pull	0-FED-1 060619	
Informati on Exposure	30-05-	2019	4.7	Samplin (MDSUM memory micropr	roarchitectural Data pling Uncacheable Memory SUM): Uncacheable nory on some coprocessors utilizing culative execution may			https://w.inte /conte ww/u securi	l.com ent/w s/en/ ty-	O-FED-1 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	sh Date	cvss	D	escription	n & CVE II	D	Pat	tch	NCIIP	CID
				allow and potential disclosuluments information guidance CVE ID:	le inforrside cha s. A list octs can b tel.com/ iblic/us, rate- 00233- te- 019.pdf	nation nnel of oe 'conten /en/do	sory/i sa- 00233				
four-faith											
f3x24_firm	iware										
Improper Neutraliz ation of Special Elements used in a Comman d ('Comma nd Injection' )	17-05	-2019	9	Four-Fai Router F allow re via the C Adminis screen.	3x24 v1 mote co comman tration >	0 devic de execu d Shell ( > Comm	es ition aka ands)	N/A		O-FOU- 060619	
Intel											
pentium_s	ilver_n	5000_fi	rmwai	re							
Improper Access Control	17-05	-2019	2.1	Insuffici vulneral reference Pentium Intel(R) N Series Series, In Series, In Processo Atom(R)	silicon are for I cessor J cessor J (R) Pro Celero Celeron( Atom(R) es, Intel	ntel(R) Series, cessor n(R) J R) N	N/A		0-INT-I 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Series, 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		
microarch	itectural_data	_sampl	ling_uncacheable_memory_firmv	ware	
Informati on 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/conten t/dam/www/public/us/en/do cuments/corporate- information/SA00233- microcode-update- guidance_05132019.pdf  CVE ID: CVE-2019-11091	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00233.html	O-INT-MICR- 060619/1113
nuc_kit_fir	mware				
Improper Input Validatio n	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_ex	recution_engin	e_firm	ware		
N/A	17-05-2019	4.6	Insufficient access control	N/A	O-INT-TRUS-
CV Scoring (CVSS)	()-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	1	NCIIPC ID
			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_man	ageme	ent_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.	N/A		O-INT-CONV- 060619/1117
1 24201	C		CVE ID : CVE-2019-0098			
Improper Restrictio n of Operatio ns 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
CV Scoring	Scale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	)	NCIIPC ID
			service via local access.			
			CVE ID : CVE-2019-0119			
hns2600b	pb24_firmwar	e				
Improper Restrictio n of Operatio ns 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
hns2600b	pb_firmware					
Improper Restrictio n of Operatio ns 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
hns2600b	pblc24_firmwa	are				
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish	Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
Buffer				privilege	-		of				
				service v							
				CVE ID :	CVE-20	19-011	9				
hns2600b	pblc_firm	iware									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2	019	7.2	Buffer or system for Xeon(R) Intel(R) Processor Board, Intel and Inter may allo potential privilege service v  CVE ID:	irmware Process Xeon(R) or, Intel( ntel(R) S l(R) Con w a priv lly enable and/or via local	e for Inte or D Far Scalabl R) Serve erver Sy npute M ileged u le escala denial c access.	el(R) mily, e er vstem odule ser to tion of	N/A		0-INT-I 060619	_
hns2600b	pq24_fir	mwar	e								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2	019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilege	offer overflow vulnerability in stem firmware for Intel(R) on(R) Processor D Family, tel(R) Xeon(R) Scalable ocessor, Intel(R) Server eard, Intel(R) Server System d Intel(R) Compute Module ay allow a privileged user to tentially enable escalation of ivilege and/or denial of rvice via local access.					0-INT-I 060619	
hns2600b	pq_firmv	vare									
Improper Restrictio n of Operatio ns within the Bounds of a	17-05-2	019	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		0-INT-I 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	& CVE II	)	Pat	ch	NCIIP	CID
Memory Buffer				potentia privilege service v	e and/or via local	denial o	of				
hns2600bj	ps24_fi	rmwar	e								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	Buffer of system for Xeon(R) Intel(R) Processor Board, Intel and Intel may allo potential privilege service v  CVE ID:	irmware Process Xeon(R) or, Intel( ntel(R) Son W a prive lly enable and/or via local	e for Inte or D Far Scalabl R) Server Server Sy apute M rileged u le escala denial d access.	el(R) mily, e er ystem odule ser to etion of	N/A		O-INT-I 060619	_
hns2600bj	ps_firm	ıware									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05·		7.2	Buffer or system for Xeon(R) Intel(R) Processor Board, Intel and Intel may allo potential privilege service v  CVE ID:	irmware Process Xeon(R) Or, Intel( ntel(R) Son W a prive Elly enable and/or via local	e for Inte or D Far Scalabl R) Server Server Sy apute M rileged u le escala denial d access.	el(R) mily, e er ystem odule ser to etion of	N/A		O-INT-I 060619	
hns2600jf	_firmw	are									
Improper Restrictio n of Operatio ns within the Bounds	17-05	-2019	7.2	Buffer or system f Xeon(R) Intel(R) Processo Board, In and Inte	irmware Process Xeon(R) or, Intel( ntel(R) S	e for Inte or D Far Scalabl R) Serve Server Sy	el(R) mily, e er ystem	N/A		0-INT-I 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch	NCIIP	C ID
of a Memory Buffer			may allo potentia privilege service v	lly enable and/or	le escala denial c	tion of				
			CVE ID :	CVE-20	19-011	9				
hns2600jf	f_firmware									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer or system f Xeon(R) Intel(R) Processor Board, In and Inte may allo potentia privilege service v	irmware Process Xeon(R) or, Intel( ntel(R) S l(R) Com ow a priv lly enable and/or via local	e for Inte or D Far Scalable R) Serve erver Sy apute Me ileged u le escala denial c access.	el(R) mily, e er vstem odule ser to tion of	N/A		0-INT-H 060619	
hns2600if	q_firmware		01212							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilego service v	overflow vulnerability in firmware for Intel(R)  Processor D Family, Xeon(R) Scalable or, Intel(R) Server ntel(R) Server System el(R) Compute Module ow a privileged user to ally enable escalation of e and/or denial of via local access.  : CVE-2019-0119			N/A		0-INT-H 060619	
hns2600k	p_firmware									
Improper Restrictio n of Operatio ns within the	17-05-2019	7.2	system f Xeon(R) Intel(R) Processo	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					0-INT-H 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	a & CVE II	D	Pat	ch	NCIIP	CID
Bounds of a Memory Buffer				and Inte may allo potentia privilege service v	ow a priv lly enab e and/or via local	rileged u le escala denial d access.	ser to ation of of				
hns2600k	pf_firm	ware									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	Buffer of system for Xeon(R) Intel(R) Processor Board, Intel and Intel may allo potential privilege service versions.	irmware Process Xeon(R) Or, Intel( ntel(R) S I(R) Con w a priv Ily enab e and/or via local	e for Integral Fail (Scalable R) Server Sympute Merileged unle escalable denial caccess.	el(R) mily, e er ystem odule eser to ation of	N/A		O-INT-H 060619	
hns2600k	pfr_firr	nware									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05		7.2	Buffer of system for Xeon(R) Intel(R) Processor Board, Intel and Intel may allo potential privilege service of CVE ID:	irmware Process Xeon(R) Or, Intel( ntel(R) S I(R) Con w a priv Ily enab e and/or via local	e for Integral Fail (Scalable R) Server Sympute Merileged unle escalable denial caccess.	el(R) mily, e er ystem odule eser to ation of	N/A		O-INT-H 060619	
hns2600k	pr_firm	iware									
Improper Restrictio n of Operatio ns within	17-05	-2019	7.2	system f Xeon(R) Intel(R)	er overflow vulnerability in em firmware for Intel(R) a(R) Processor D Family, (R) Xeon(R) Scalable essor, Intel(R) Server					0-INT-I 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
the Bounds of a Memory Buffer			Board, In and Inte may allo potentia privilege service v	l(R) Conow a privolent lly enable and/or via local	npute M rileged u le escala denial d access.	odule ser to ition of of				
hns2600tr	24r_firmwar	Δ	CVE ID :	CVE-ZU	19-011	9				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer of system for Xeon(R) Intel(R) Processor Board, Intel and Intel may allo potential privilege service v  CVE ID:	irmware Process Xeon(R) Or, Intel( ntel(R) S I(R) Con w a priv lly enab e and/or via local	e for Inte or D Far Scalabl R) Server Server Sy apute M rileged u le escala denial d access.	el(R) mily, e er ystem odule ser to ition of	N/A		O-INT-H 060619	
hns2600tr	024sr_firmwa	re	CVL ID.	CVL 20	17 011					
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilege	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		0-INT-H 060619	
hns2600tp	24str_firmwa	are	CVE ID . CVE 2017 0117							
Improper Restrictio n 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		0-INT-H 060619		
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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	o_firmware				
Improper Restrictio n of Operatio ns 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	0-INT-HNS2- 060619/1137
hns2600tp	of_firmware				
Improper Restrictio n of Operatio ns 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
hns2600tr	ofr_firmware				
Improper Restrictio n 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	C ID
Operatio ns within the Bounds of a Memory Buffer			and Inte may allo potentia privilego	or, Intel( ntel(R) S l(R) Com ow a priv llly enabl	R) Serve erver Sy ipute M ileged u le escala denial d	er ystem odule ser to ition of				
1 2600	C		CVE ID : CVE-2019-0119							
hns2600tp	onr_firmwar	е								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  System Xeon( Intel(I Proces Board and In may a potent privile service				verflow y firmware Process Xeon(R) or, Intel( ntel(R) S el(R) Com ow a privally enable e and/or via local	e for Inte or D Far Scalabl R) Serve erver Sy pute M ileged u le escala denial d access.	el(R) mily, e er ystem odule ser to ution of	N/A		0-INT-H 060619	
hns2600tp	or_firmware		•							
Improper Restrictio n of Operatio ns 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		0-INT-H 060619	
hns2600w	p_firmware									
Improper Restrictio	17-05-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)				N/A		0-INT-H 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
n of Operatio ns 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		
hns2600w	pf_firmware	1			
Improper Restrictio n of Operatio ns 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
hns2600w	pq_firmware				
Improper Restrictio n of Operatio ns 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
hns7200aj	p_firmware	u			
Improper	17-05-2019	7.2	Buffer overflow vulnerability in	N/A	O-INT-HNS7-
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Restrictio n of Operatio ns 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
hns7200aj	pl_firmware				
Improper Restrictio n of Operatio ns 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
hns7200aj	pr_firmware				
Improper Restrictio n of Operatio ns 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
hns7200aj	prl_firmware				1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restrictio n of Operatio ns 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
mfs2600k	i_firmware				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	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-MFS2- 060619/1149
mfs5000si	i_firmware				
Improper Restrictio n of Operatio ns 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

CV Scoring Scale	0-1	1_2	2-3	2-1	<b>1</b> -5	5-6	6-7	7₋0	8-9	0_10
(CVSS)	0-1	1-2	2-3	3-4	4-5	3-0	0-7	7-0	0-9	3-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mfs5520v	ir_firmware				_
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	may allow a privileged user to potentially enable escalation of privilege and/or denial of service via local access.  CVE ID: CVE-2019-0119  o_firmware		N/A	0-INT-MFS5- 060619/1151
server_boa	ard_s1200sp_f	irmwa	re		
Improper Restrictio n of Operatio ns 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_boa	ard_s2600bp_f	irmwa	re		
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	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	Pat	tch	NCIIPC ID
			CVE ID : CVE-2019-0119			
server_boa	ard_s2600cw_f	firmwa	ire			
Improper Restrictio n of Operatio ns 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_boa	ard_s2600kp_f	irmwa	re	•		
Improper Restrictio n of Operatio ns 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		0-INT-SERV- 060619/115!
server_boa	ard_s2600st_fi	rmwar	re			
Improper Restrictio n of Operatio ns 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		0-INT-SERV- 060619/1150
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	D	escription	a & CVE II	D	Pat	tch	NCIIP	C ID
				service v	ia local	access.					
				CVE ID :	CVE-20	19-011	9				
server_boa	ard_s20	600tp_fi	rmwai	re							
Improper Restrictio n of Operatio ns 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  re				N/A		O-INT-S 060619	
server_boa	ard_s2	600wf_f	irmwa	re							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilego service v	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					0-INT-9 060619	
server_boa	ard_s2	600wt_f	irmwa	re							
Improper Restrictio n of Operatio ns 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-S 060619		
CV Scoring (CVSS)	CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10			

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	CID
Buffer			privilege	•		of				
			service v	<i>i</i> a local	access.					
			CVE ID :	CVE-20	19-011	9				
server_boa	ard_s7200ap_1	irmwa	re							
Improper Restrictio n of Operatio ns 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		0-INT-S 060619	
server_sys	tem_s9200wk	_firmw	are							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilege service v	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					O-INT-S 060619	
xeon_bron	ze_processors	_firmv	vare							
Improper Restrictio n of Operatio ns 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		0-INT-X 060619	
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish	h Date	CVSS	D	escriptio	n & CVE I	D	Pat	tch	NCIIP	C ID
Memory Buffer				potential privilego service v	e and/or via local	denial (	of				
N/A	17-05-	2019	7.2	Insuffici silicon r Intel(R) Processo privilego enable e and/or o local acc	eference Xeon(R) or, Intel( or D Fan ed user to escalation denial of cess.	e firmwa Scalabl (R) Xeon nily may to poten n of priv Service	re for e (R) allow a tially ilege via	N/A		O-INT-X 060619	
xeon_d-16	02_firm	ıware		0.212							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-		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		0-INT-X 060619	
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		0-INT-X 060619	
xeon_d-16	xeon_d-1622_firmware										
CV Scoring	Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restrictio n of Operatio ns 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-16	23n_firmware				
Improper Restrictio n of Operatio ns 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-XEON- 060619/1168
			<b>CVE ID : CVE-2019-0119</b>		
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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
			Processo privilege enable e and/or o local acc	ed user to scalation lenial of ess.	o potent of priv service	ially ilege via				
xeon_d-16	27_firmware									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2019	7.2	Buffer or system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilege service v	irmware Process Xeon(R) or, Intel( ntel(R) S I(R) Com w a priv Ily enable and/or via local	e for Inte or D Far Scalabl R) Serve erver Sy apute M ileged u e escala denial d access.	el(R) mily, e er ystem odule ser to ction of	N/A		O-INT-X 060619	
			CVE ID :							
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.				N/A		0-INT-X 060619	
	22 C*		CVE ID :	CVE-20	19-012	6				
xeon_d-16 Improper	33n_firmware		Ruffer	verflow	nilneral	nility in				
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-X 060619		
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish D	ate C	CVSS	Description & CVE ID			Patch		NCIIPC ID		
Buffer				privilege and/or denial of service via local access.							
				CVE ID:	CVE-20	19-011	.9				
N/A	17-05-20	19 7	'.2	Insufficion resilicon relation (R) Processo privilego enable e and/or o local accompany	eference Xeon(R) or, Intel( or D Famed user to scalation denial of ess.	e firmwa Scalabl R) Xeon nily may to poten n of priv Service	re for e (R) allow a tially rilege via	N/A		O-INT-> 060619	
				CVE ID :	CVE-20	19-012	6				
xeon_d-16	37_firmwa	are									
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-20	19 7	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-> 060619	
N/A	17-05-2019 7.2		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	r 17-05-2019 <b>7</b>		7.2	Buffer overflow vulnerability in			N/A		O-INT-XEON-		
CV Scoring Scale (CVSS) 0-1		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
Restrictio n of Operatio ns 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-16	53n_firmware					
Improper Restrictio n of Operatio ns 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-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	
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publis	h Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
				privilege enable e and/or o local acc	scalation denial of	n of priv	ilege				
				CVE ID : CVE-2019-0126							
xeon_d-21	23it_fiı	rmware									
Improper Restrictio n of Operatio ns 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-X 060619	
				CVE ID :	CVE-20	19-011	9				
N/A	17-05	-2019	7.2	silicon re Intel(R) Processo Processo privilege enable e and/or o local acc	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					O-INT-X 060619	_
xeon_d-21	41i_fir	mware									
Improper Restrictio n of Operatio ns 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-X 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pa	tch	NCIIP	C ID
Buffer				service v	via local	access.					
				CVE ID	CVE-20	19-011	.9				
N/A	17-05	-2019	7.2	Insuffici silicon r Intel(R) Processo Processo privilego enable e and/or o local acc	eference Xeon(R) or, Intel( or D Fan ed user t escalation denial of cess.	e firmwa ) Scalabl (R) Xeon nily may to poten n of priv Service	re for e (R) allow a tially rilege via	N/A		0-INT-X 060619	_
voon d 21	42i+ fir	rmwana		CVEID	CVE-ZU	119-012					
xeon_d-21	421t_III	шwаге		D. CC	<u> </u>	1	1 -11				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	system f Xeon(R) Intel(R) Processe Board, I and Inte may allo potentia privilege	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.					0-INT-X 060619	
N/A	17-05	-2019	7.2	Insufficisilicon r Intel(R) Processo Processo privilego enable e and/or o local acco	ent acce eference Xeon(R) or, Intel( or D Fan ed user t escalation denial of	ss contrestimmants  Scalable  (R) Xeonally may  so potenate  n of prive  service	ol in are for e (R) allow a tially rilege via	N/A		0-INT-X 060619	
xeon_d-21	43it_fii	rmware									
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)  N/A  0-INT-XE 060619/1							
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
n of Operatio ns 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-21	45nt_firmwar	e			
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7	<b>7-8 8-9 9-10</b>

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-21	46nt_firmwar	e			
Improper Restrictio n of Operatio ns 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-21	61i_firmware				
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
				service v	via local	access.					
				CVE ID	CVE-20	19-011	.9				
N/A	17-05	-2019	7.2	Insuffici silicon r Intel(R) Processo privilego enable e and/or o local acc	eference Xeon(R) or, Intel( or D Fan ed user to escalation denial of cess.	e firmwa ) Scalabl (R) Xeon nily may to poten n of priv Service	are for e (R) allow a tially vilege via	N/A	/A 0-INT-XE0 060619/11		_
woon d 21	62i+ fix	um III a no		CVEID	CVE-ZU	119-012	.0				
xeon_d-21	osit_Ill	mware		D CC	C	1	1 .1				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	system f Xeon(R) Intel(R) Processe Board, I and Inte may allo potentia privilege service v	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		0-INT-X 060619	
N/A	17-05	-2019	7.2	Insuffici silicon r Intel(R) Processo privilego enable e and/or o local acc	ent acce eference Xeon(R) or, Intel( or D Fan ed user t escalation denial of	ss contrestimmants  Scalable  (R) Xeonally may  so potenate  n of prive  service	ol in are for e (R) allow a tially vilege via	N/A		0-INT-X 060619	
xeon_d-21	66nt_fi	firmware									
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)  N/A  0-INT-XEO 060619/11							
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch		NCIIPC ID
n of Operatio ns 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-21	73it_firmware				•	
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9 9-10

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-21	77nt_firmwar	e			
Improper Restrictio n of Operatio ns 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-XEON- 060619/1200
			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.	N/A	O-INT-XEON- 060619/1201
			CVE ID : CVE-2019-0126		
xeon_d-21	83it_firmware				
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				service v	⁄ia local	access.					
				CVE ID:	CVE-20	19-011	9				
N/A	17-05	-2019	7.2	Insuffici silicon rule (R) Processo processo privilege enable e and/or o local acc	eference Xeon(R) or, Intel( or D Fam ed user t scalation denial of	firmwa Scalabl R) Xeon aily may o potent a of priv	re for e (R) allow a cially ilege	N/A		0-INT-X 060619	_
				CVE ID:	CVE-20	19-012	6				
xeon_d-21	87nt_fi	rmware	e								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilege	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.					0-INT-X 060619	
N/A	17-05	-2019	7.2	Insuffici silicon runtel(R) Processo privilego enable e and/or o local aco	ent accest eference Xeon(R) or, Intel( or D Famed ed user t scalation denial of	ss control firmwa Scalabl R) Xeon tily may o potent n of priv service	ol in re for e (R) allow a cially ilege via	N/A		0-INT-X 060619	
xeon_d-21	91_firn	nware									
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)  O-INT-XEO 060619/1							
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
n of Operatio ns 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_fi	rmwar	e		
Improper Restrictio n of Operatio ns 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	0-INT-XEON- 060619/1209
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7	7-8 8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access.		
			CVE ID: CVE-2019-0126		
xeon_plati	num_processo	rs_firn	nware		
Improper Restrictio n of Operatio ns 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.	N/A	O-INT-XEON- 060619/1211
woon nnog	oggon d 1512r	, finns	CVE ID : CVE-2019-0126		
_	essor_d-15131	1_1111111			
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				service v	ia local	access.					
				CVE ID:	<b>CVE-20</b>	19-011	9				
N/A	17-05	-2019	7.2	Insuffici silicon rule (R) Processo processo privilege enable e and/or o local acc	eference Xeon(R) or, Intel( or D Fam ed user t scalation denial of	firmwa Scalabl R) Xeon aily may o potent a of priv	re for e (R) allow a cially ilege	N/A	N/A O-INT-XEO 060619/1		_
				CVE ID :	CVE-20	19-012	6				
xeon_proc	essor_c	l-1518_	firmwa	are							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilege	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.					0-INT-X 060619	
N/A	17-05	-2019	7.2	Insuffici silicon runtel(R) Processo privilege enable e and/or o local acco	ent accese eference Xeon(R) or, Intel( or D Famed user t ed user t scalation denial of	ss control firmwa Scalabl R) Xeon fily may o potent of prive service	ol in re for e (R) allow a cially ilege via	N/A		0-INT-X 060619	
xeon_proc	essor_c	l-1520_	firmwa	are							
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)  N/A  0-INT-XEO 060619/12							
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish	Date	CVSS	D	escription	a & CVE II	)	Pat	ch	NCIIP	C ID
n of Operatio ns within the Bounds of a Memory Buffer				Intel(R) Processo Board, In and Inte may allo potentia privilege service v	R) Processor D Family, R) Xeon(R) Scalable ssor, Intel(R) Server , Intel(R) Server System tel(R) Compute Module low a privileged user to cially enable escalation of ege and/or denial of e via local access. D: CVE-2019-0119						
N/A	17-05-2		7.2	Insuffici silicon rulle (R) Processo privilego enable e and/or o local acc	eference Xeon(R) or, Intel( or D Fam ed user t scalation denial of	firmwa Scalabl R) Xeon aily may o potent of priv service	re for e (R) allow a tially ilege via	N/A		0-INT-X 060619	_
xeon_proc	essor_d-	1521_	firmwa	are							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05-2	2019	7.2	system f Xeon(R) Intel(R) Processo Board, In and Inte may allo potentia privilege service v	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		0-INT-X 060619	
N/A	17-05-2	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		0-INT-X 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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_proc	essor_d-15231	n_firmv	vare		
Improper Restrictio n of Operatio ns 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-XEON- 060619/1220
			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.	N/A	O-INT-XEON- 060619/1221
			CVE ID : CVE-2019-0126		
xeon_proc	essor_d-1527_	firmwa	are		
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	C ID
				service via local access.							
				CVE ID : CVE-2019-0119							
N/A	17-05	-2019	7.2	silicon r Intel(R) Processo Processo privilego enable e and/or o	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.					0-INT-X 060619	_
				CVE ID	: CVE-20	19-012	26				
xeon_proc	essor_c	l-1528_	firmwa	are							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	Buffer of system for Xeon(R) Intel(R) Processor Board, If and Interpretation potential privilegors of the service of the system	irmward Process Xeon(R) or, Intel( ntel(R) Son ow a privally enab e and/or via local	e for Integer D Far Sor D Far Server Sympute M Vileged U le escala denial daccess.	el(R) mily, e er ystem odule aser to ation of	N/A		0-INT-X 060619	
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		0-INT-X 060619		
xeon_proc	essor_c	l-1529_	firmwa	are							
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)			N/A		0-INT-X 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	l	NCIIPC ID
n of Operatio ns 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		0-INT-XEON- 060619/1227
xeon_proc	essor_d-1531_	firmw	are			
Improper Restrictio n of Operatio ns 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		0-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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

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_proc	essor_d-15331	n_firmv	vare		
Improper Restrictio n of Operatio ns 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-XEON- 060619/1230
			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.	N/A	O-INT-XEON- 060619/1231
			CVE ID : CVE-2019-0126		
xeon_proc	essor_d-1537_	firmwa	are		
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	C ID
				service via local access.							
				CVE ID : CVE-2019-0119							
N/A	17-05	-2019	7.2	silicon r Intel(R) Processo Processo privilego enable e and/or o local acc	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					0-INT-X 060619	_
					CVE-20	19-012	6				
xeon_proc	essor_c	1-1539_	firmwa								
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	Buffer of system for Xeon(R) Intel(R) Processor Board, I and Interpretation potential privilegor service of the system of the sy	irmward Process Xeon(R) or, Intel( ntel(R) Son ow a privally enab e and/or via local	e for Integral of Far (Server Sympute Marileged unless allowed allowed allowed allowed access.	el(R) mily, e er ystem odule aser to ation of	N/A		0-INT-X 060619	
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		0-INT-X 060619		
xeon_proc	essor_c	l-1540_	firmwa	are							
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)			N/A		0-INT-X 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
n of Operatio ns 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_proc	essor_d-1541_	firmw	are		
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7	'-8 8-9 <b>9-10</b>

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 Restrictio n of Operatio ns 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				
voon nroc	occor d 1540	firmy							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	essor_d-1548_ 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				
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publis	h Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	C ID
				service via local access.							
				CVE ID:	CVE ID : CVE-2019-0119						
N/A	17-05	-2019	7.2	silicon r Intel(R) Processo Processo privilego enable e and/or o	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.					O-INT-X 060619	
				CVE ID :	CVE-20	19-012	6				
xeon_proc	essor_c	d-1553r	_firmv	ware							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	Buffer of system for Xeon(R) Intel(R) Processor Board, Intel and Intel may allo potential privilege service v	irmware Process Xeon(R) Or, Intel( ntel(R) S I(R) Con w a priv Ily enab e and/or via local	e for Inte or D Far Scalabl R) Serve Server Sy apute M rileged u le escala denial c access.	el(R) mily, e er vstem odule ser to tion of	N/A		0-INT-X 060619	
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-X 060619		
xeon_proc	essor_c	d-1557_	firmwa	iware							
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)			N/A		0-INT-X 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
n of Operatio ns 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_proc	essor_d-1559_	firmw	are		
Improper Restrictio n of Operatio ns 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	0-INT-XEON- 060619/1249
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	1	NCIIPC ID
			enable escalation of privilege and/or denial of service via local access.			
			<b>CVE ID : CVE-2019-0126</b>			
xeon_proc	essor_d-1567_	firmwa	are			
Improper Restrictio n of Operatio ns 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-XEON- 060619/1250
			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.	N/A		O-INT-XEON- 060619/1251
			CVE ID : CVE-2019-0126			
xeon_proc	essor_d-1571_	firmwa	are			
Improper Restrictio n of Operatio ns 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		0-INT-XEON- 060619/1252
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publis	h Date	cvss	Description & CVE ID				Pat	tch	NCIIP	C ID
				service via local access.							
				CVE ID:	CVE ID : CVE-2019-0119						
N/A	17-05	-2019	7.2	silicon r Intel(R) Processo Processo privilego enable e and/or o	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.					0-INT-X 060619	
				CVE ID :	CVE-20	19-012	6				
xeon_proc	essor_c	d-1577_	firmw	are							
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	17-05	-2019	7.2	Buffer of system f Xeon(R) Intel(R) Processor Board, In and Intel may allo potential privilege service v	irmware Process Xeon(R) or, Intel( ntel(R) S l(R) Con w a priv lly enab e and/or via local	e for Inte or D Far Scalabl R) Server Server Sy apute M rileged u le escala denial c access.	el(R) mily, e er vstem odule ser to tion of	N/A		0-INT-X 060619	
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-X 060619		
xeon_silve	r_proc	essors_f	firmwa	ire							
Improper Restrictio	17-05	-2019	7.2	Buffer overflow vulnerability in system firmware for Intel(R)				N/A		0-INT-X 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Operatio ns 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	D	escription	& CVE II	)	Pat	ch:	NCIIP	C ID								
Improper Access Control	17-05-2019	2.1	reference Pentium Intel(R) N Series, In Series, In Processo Atom(R) Series, In Processo allow a p potential service v	entium(R) Processor J Series, tel(R) Pentium(R) Processor Series, Intel(R) Celeron(R) Jeries, Intel(R) Celeron(R) Neries, Intel(R) Atom(R) Processor A Series, Intel(R) Com(R) Processor E3900 Pries, Intel(R) Pentium(R) Processor Silver Series may low a privileged user to obtentially enable denial of rvice via local access.				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				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.					0-INT- <i>A</i> 060619	
atom_x5-e	3930_firmwa	re																
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- <i>A</i> 060619											
atom_x5-e	3940_firmwa	re																
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		0-INT- <i>A</i> 060619									
CV Scoring (CVSS)		1-2	2-3	3-4 4-5 5-6		6-7	7-8	8-9	9-10									

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			N 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-e	3950_firmwar	e			
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_j3	060_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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			Series, In Processor allow a potential service v	or Silver privilege illy enab via local	Series n d user to le denial access.	nay o l of				
celeron_j3	160_firmware									
Improper Access Control	17-05-2019	2.1	Insufficition vulneral reference Pentium Intel(R) N Series, In Series, In Processor Atom(R) Series, In Processor allow a potential service version of the control of the co	ce firmware	silicon are for Is cessor J S a(R) Pro- Celeron(Celeron(R) es, Inteles cor E390 Pentium Series n d user to le denial access.	ntel(R) Series, cessor n(R) J R) N (R) 00 (R) nay o	N/A		O-INT-0 060619	
celeron_j3	355_firmware						<u> </u>			
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-0 060619	
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish	n Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				CVE ID :	CVE-20	19-012	0				
celeron_j3	455_fir	mware									
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		0-INT-0 060619	
celeron_j4	005_fir	mware									
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-0 060619	
celeron_j4	105_fir	mware									
Improper Access	17-05-	2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(R)				N/A		O-INT-0 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	<b>2-3</b> 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	tch	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_n2	2830_firmwar	e				
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 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_n2	2840_firmwar	e				
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
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escriptio	n & CVE I	D	Pat	tch	NCIIP	CID
celeron na	2930_firmwar	e	Processor Atom(R) Series, II Processor allow a potential service v CVE ID	) Proces ntel(R) I or Silver privilege ally enab via local	Pentium Pentium Series red user ted users.	00 (R) nay o l of				
celefon_nz	2750_III III war		I				T		I	
Improper Access Control	Insufficition vulneral reference Pentium Intel(R) N Series, Intel(R) Series, Interessed Atom(R) Series, Interessed Atom(R) Series, Interessed Atom(R) Series, Interessed Atom(R) CVE ID:	bility in a ce firmw (R) Procesor A Serior Silver privilege (ally enably in a firm a f	silicon are for I cessor J n(R) Pro Celeron( Atom(R) es, Intel sor E390 Pentium Series r ed user t le denia access.	ntel(R) Series, cessor n(R) J R) N  (R) 00 (R) nay o	N/A		O-INT-0 060619			
celeron_n2	2940_firmwar	e					•			
Improper Access Control	17-05-2019	2.1	Insufficition vulneral reference Pentium Intel(R) N Series, Intel Series, Intel Processe Atom(R) Series, Intel Processe Atom(R) Series, Intel Processe Atom (R) Series, Intel Processe Atom (R)	bility in a ce firmw (R) Prod Pentium (Intel(R) (Intel(R) A or A Seri (I) Proces (I) Proces (I) Proces (II) Intel(R) Int	silicon are for I cessor J n(R) Pro ) Celeron Celeron(R) des, Intel sor E390 Pentium Series r	ntel(R) Series, cessor n(R) J R) N (R) 00 (R) nay	N/A		0-INT-0 060619	
CV Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

celeron_n3000_firmware    Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor   Series, Intel(R) Celeron(R)   Series, Intel(R) Pentium(R) Processor   Series, Intel(R)   Se	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
COLETON_03000_firmware  Improper Access Control  Improper Access Contro				*						
Improper Access Control  Improper Access Contr				service via local access.						
Improper Access Control   17-05-2019   17-05-2019   2.1   Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Celeron(R) J Series, Intel(R) Celeron(R) N Series, Intel(R) Celeron(R) N Series, Intel(R) Processor A Series, Intel(R) Processor E3900 Series, Intel(R) Processor E3900 Series, Intel(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access.  CVE ID : CVE-2019-0120   2.1   Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor I Series, Intel(R) Pentium(R) Processor I Series, Intel(R) Pentium(R) Processor N Series, Intel(R) Celeron(R) N Series, Intel(R) Celeron(R) N Series, Intel(R) Celeron(R) N Series, Intel(R) Atom(R) Processor E3900 Series, Intel(R) Pentium(R) Processor E3900 Series, Intel(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				CVE ID : CVE-2019-0120						
Improper Access   17-05-2019   2.1   Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Processor J Series, Intel(R) Celeron(R) J Series, Intel(R) Processor E3900 Series, Intel(R) Processor E3900 Series, Intel(R) Processor E3900 Series, Intel(R) Processor Silver Series may allow a privileged user to potentially enable denial of service via local access.    Insufficient key protection vulnerability in silicon reference firmware for Intel(R) Pentium(R) Processor J Series, Intel(R) Pentium(R) Processor E3900 Series, Intel(R) Pentium(R) Processor E3900 Series, Intel(R) Pentium(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_n3	3000_firmware	е							
Improper Access Control  Improper Access Intel(R) Pentium(R) Processor J 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	Access	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		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					
Improper Access Control  17-05-2019  2.1  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	celeron_n3	3350_firmware	9							
celeron_n3450_firmware	Improper Access Control	17-05-2019	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		N/A					
	celeron_n3	celeron_n3450_firmware								

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID			
Improper Access Control	17-05-2019	2.1	reference Pentium Intel(R) N Series Series, In Series, In Processo Atom(R) Series, In Processo allow a p potential service v	m(R) Processor J Series, c) Pentium(R) Processor es, Intel(R) Celeron(R) J Intel(R) Celeron(R) N Intel(R) Atom(R) sor A Series, Intel(R) R) Processor E3900 Intel(R) Pentium(R) sor Silver Series may a privileged user to itally enable denial of e via local access.			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		0-INT-0 060619	
celeron_n4	1000_firmwa	re											
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		0-INT-0 060619						
celeron_n4	1100_firmwa	re											
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		0-INT-0 060619				
CV Scoring (CVSS)		1-2	2-3	3-4 4-5 5-6		6-7	7-8	8-9	9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Pat	tch	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_firm	ıware					
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 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_firm	iware					
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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patc	h	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_firm	nware					
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_firi	mware			T		
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
CV Scoring (CVSS)	()-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pa	tch	NCIIP	CID
			CVE ID :	CVE-20	19-012	0				
n3540_firm	nware									
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_firm	MANANA		CVE ID.	CVE-ZU	19-012	<u> </u>				
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-N 060619	
pentium_s	ilver_j5005_fi	rmwar	e							
Improper Access	17-05-2019	2.1	Insufficient key protection vulnerability in silicon reference firmware for Intel(F				N/A		O-INT-F 060619	
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	tch	NCIIP	C 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 :	<b>CVE-20</b>	19-012	0				
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-: 060619	
Linux	a a l									
linux_kerr	lei		An issue	was die	rovered	in				
NULL Pointer Derefere nce	27-05-2019	4.9	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		0-LIN-L 060619	
CV Scoring (CVSS	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE I	D	Pat	tch	NCIIP	C ID
			an attac service ( derefere	(NULL po	ointer					
			CVE ID :	CVE-20	19-123	378				
N/A	27-05-2019	4.9	An issue con_inse drivers/ the Linu There is certain coutcome	ert_unipa /tty/vt/c x kernel a memo case of an	air in consolen through ory leak n ENOM lloc.	nap.c in n 5.1.5. in a EM	N/A		0-LIN-L 060619	
N/A	27-05-2019	2.1	An issue efi subsy kernel the phys_efi ap in arch/x8 and efi_carch/x8 mishand failures.	N/A		0-LIN-I 060619				
NULL Pointer Derefere nce	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		0-LIN-I 060619	_
NULL Pointer Derefere nce	27-05-2019	4.9	An issue drm_loa drivers/ad.c in the 5.1.5. The kstrdup	e in edid_lo through cked	N/A		0-LIN-I 060619			
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	h	NCIIPC ID
			allow an attacker to cause a denial of service (NULL pointer dereference and system crash).  CVE ID: CVE-2019-12382			
Improper Input Validatio n	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 Derefere nce	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 Validatio n	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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Microsoft					
azure_dev	ops_server_20	19			
Improper Neutraliz ation of Input During Web Page Generatio n ('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
Informati on 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 Neutraliz ation of Input During Web Page Generatio n ('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_1	10				
N/A	16-05-2019	6.9	An elevation of privilege	N/A	O-MIC-WIND-
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			vulnerability 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	erface ) when ck the rior to it.To exploit a local attacker y crafted te the level, aka vation of			
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		
CV Scoring (CVSS)	()-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10		

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.	N/A	O-MIC-WIND- 060619/1301
Informati on 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & 0	CVE ID	Pat	tch	NCIIP	C ID
			Privilege Vulnerabil	ity'.				
			CVE ID : CVE-2019-	0881				
Informati on Exposure	16-05-2019	4.3	An information disc vulnerability exists of Windows GDI comp improperly disclose contents of its memory 'Windows GDI Infort Disclosure Vulnerability CVE ID is unique from 2019-0758, CVE-20 CVE ID: CVE-2019-	when the onent s the ory, aka mation oility'. This m CVE-	N/A		O-MIC-V 060619	
Improper Input Validatio n	16-05-2019	9.3	properly validate us aka 'Windows OLE I	lity exists when Windows OLE fails to validate user input, lows OLE Remote cution Vulnerability'.			O-MIC-V 060619	
Informati on Exposure	16-05-2019	2.7	An information disc vulnerability exists of Windows Hyper-V of operating system far properly validate in authenticated user of operating system, all 'Windows Hyper-V of Disclosure Vulnerability CVE ID: CVE-2019-	N/A		O-MIC-V 060619		
Improper Restrictio n of Operatio ns within the Bounds of a Memory	16-05-2019	9.3	A remote code exectivulnerability exists windows Jet Databa improperly handles memory, aka 'Jet Da Engine Remote Code Vulnerability'. This cunique from CVE-20 CVE-2019-0891, CV 0893, CVE-2019-089	N/A		0-MIC-V 060619		
CV Scoring (CVSS)		1-2	2-3 3-4 4	-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Buffer			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 Restrictio n of Operatio ns 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-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1308
Improper Restrictio n of Operatio ns 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-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1309
N/A	16-05-2019	7.2	An elevation of privilege	N/A	O-MIC-WIND-
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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 Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1311
Improper Restrictio n of Operatio ns 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	D	escription	& CVE II	)	Pat	ch	NCIIP	C ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improperation of the window improvement of the windo	oility exics Jet Dates Jet Dates Jet Dates Jet Remote Collity'. The CVE Je-0897, JE-2019 Je-20	sts when tabase E dles object Databa Code Exc his CVE -2019-0 -0893, C -2019-0 -0899, C	N/A		0-MIC-\ 060619		
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	vulneral Window imprope memory Engine I Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0898, CV 2019-09	CVE ID: CVE-2019-0895  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-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.					0-MIC-\ 060619	
Improper Restrictio n of Operatio ns within the Bounds of a	16-05-2019	9.3	A remot vulneral Window imprope memory Engine I Vulneral unique f	N/A		O-MIC-\ 060619				
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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.		
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1316
Improper Restrictio n of Operatio ns 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	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			CVE ID :	CVE-20	19-089	9				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improper memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0897, CV 2019-08 CVE-201	oility exists Jet Dates Je	sts when abase E lles obje Databa Code Exe nis CVE -2019-0 -0893, C -2019-0 CVE-20 -0898, C	N/A		O-MIC-\ 060619		
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improper memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0897, CV 2019-08 CVE-201 CVE ID:	CVE ID: CVE-2019-0900  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-2019-0902.					O-MIC-\ 060619	
Improper Restrictio n of Operatio ns within the Bounds	16-05-2019	9.3	A remote vulneral Window imprope memory Engine F	N/A		O-MIC-\ 060619				
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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.		
Improper Restrictio n of Operatio ns 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  An elevation of privilege	N/A	0-MIC-WIND- 060619/1323
N/A	16-05-2019	2.1	vulnerability exists in the Unified Write Filter (UWF)	N/A	0-MIC-WIND- 060619/1324
CV Scoring (CVSS)	()-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

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		
Informati on 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	7				
Improper Input Validatio n	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		O-MIC-WIND- 060619/1327
N/A	16-05-2019	9.3	An elevation of privilege	N/A	O-MIC-WIND-
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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.		060619/1328
Informati on 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
Informati on 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-0758, CVE-2019-0961.		
			CVE ID : CVE-2019-0882		
Improper Input Validatio n	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 Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1333
Improper Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0900, CVE-2019-0901, CVE-2019-0902. CVE ID : CVE-2019-0890		
Improper Restrictio n of Operatio ns 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-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1335
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1336
Improper Restrictio n 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

3-4

2-3

1-2

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	ch	NCIIP	C ID
ns within the Bounds of a Memory Buffer			memory Engine I Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 CVE-201	Remote (bility'. Tl From CVE 19-0890, /E-2019 895, CVE 19-0897, /E-2019 900, CVE 19-0902.	Code Execution Execution CVE-2019-0  CVE-20  CVE-20  CVE-20  -0899, C  -2019-0	ecution ID is 1889, 19- VE- 896, 19- VE- 901,				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	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-V 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	CVE ID: CVE-2019-0895  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-V 060619	
CV Scoring (CVSS		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0901, CVE-2019-0902.  CVE ID: CVE-2019-0897	N/A	O-MIC-WIND- 060619/1340
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1341
Improper Restrictio n 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
Operatio ns within the Bounds of a Memory Buffer			imprope memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 CVE-201 CVE-201	r, aka 'Jet Remote ( bility'. Tl From CVF 19-0890, /E-2019 19-0896, /E-2019 19-0902.	Databa Code Exe his CVE -2019-0 -0893, C -2019-0 CVE-20 -0898, C	se ecution ID is 0889, 19- EVE- 895, 19- EVE- 901,				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	vulneral Window imprope memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0897, CV 2019-08	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		0-MIC-V 060619	
Improper Restrictio n of Operatio ns 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-\ 060619		
CV Scoring (CVSS)	( )- (	1-2	2-3	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-2019-0896, CVE-2019- 0897, CVE-2019-0898, CVE- 2019-0899, CVE-2019-0900, CVE-2019-0902. CVE ID: CVE-2019-0901		
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901.	N/A	O-MIC-WIND- 060619/1345
Improper Restrictio n of Operatio ns 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0936		
Informati on 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	O-MIC-WIND- 060619/1348	
windows_8	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	0-MIC-WIND- 060619/1351
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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			
Informati on 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
Informati on 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
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validatio n	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 Restrictio n of Operatio ns 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-2019-0897, CVE-2019-0890, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1356
Improper Restrictio n of Operatio ns 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-2019-0901, CVE-2019-0902.  CVE ID: CVE-2019-0890	N/A	O-MIC-WIND- 060619/1357

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	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-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.  CVE ID: CVE-2019-0891  A remote code execution				N/A		0-MIC-\ 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3					N/A		0-MIC-\ 060619	
Improper Restrictio n of Operatio ns 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-\ 060619	
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0890, CVE-2019-0891, CVE-2019-0893, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.		
			CVE ID : CVE-2019-0894		
Improper Restrictio n of Operatio ns 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- 060619/1361
			CVE ID : CVE-2019-0895		
Improper Restrictio n of Operatio ns 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-2019-0897, 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	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			CVE ID :	CVE-20	19-089	6				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improper memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0898, CV 2019-09 CVE-201	oility exists Jet Dates Je	sts when abase E lles obje Databa Code Exe nis CVE -2019-0 -0893, C -2019-0 CVE-20 -0899, C	n the ngine cts in se ecution ID is 19-VE-895, 19-VE-901,	N/A		O-MIC-\ 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improper memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0897, CV 2019-09 CVE-201 CVE ID:	CVE ID: CVE-2019-0897  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-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.  CVE ID: CVE-2019-0898					O-MIC-\ 060619	
Improper Restrictio n of Operatio ns within the Bounds	16-05-2019	9.3	A remote vulneral Window imprope memory Engine F	oility exists Jet Date of Part Part Part Part Part Part Part Part	sts wher abase E lles obje Databa Code Exe	n the ngine cts in se ecution	N/A		O-MIC-\ 060619	
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Descrip	tion & CVE I	D	Pat	tch	NCIIP	CID
of a Memory Buffer			unique from CVE-2019-08 0891, CVE-20 2019-0894, C CVE-2019-08 0897, CVE-20 2019-0900, C CVE-2019-09	390, CVE-20 319-0893, C 3VE-2019-0 396, CVE-20 319-0898, C 3VE-2019-0	019- CVE- 895, 019- CVE-				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code vulnerability Windows Jet improperly homemory, aka Engine Remo Vulnerability unique from CVE-2019-08 0891, CVE-2019-08 0897, CVE-2019-0899, CVE-2019-099 CVE ID : CVE	e execution exists when the code Exists when the code Exists Exists and the code Exists CVE-2019-0396, CVE-2019-0396, CVE-2019-0302.	n the ngine ects in se ecution ID is 0889, 019-CVE-019-CVE-0901,	N/A		O-MIC-V 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote cod vulnerability Windows Jet improperly h memory, aka Engine Remo Vulnerability unique from CVE-2019-08 0891, CVE-2019-08 0897, CVE-2019-08 0897, CVE-2019-0899, CVE-2019-0899, CVE-2019-0899	exists when Database E andles object Database E de Code Except CVE-2019-0393, CVE-2019-0396, CVE	n the ngine ects in se ecution ID is 0889, 019-CVE-895, 019-CVE-CVE-	N/A		0-MIC-V 060619	
CV Scoring (CVSS)	()-	1-2	2-3 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-2019-0901		
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1368
Improper Restrictio n of Operatio ns 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
Informati on Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	0-MIC-WIND- 060619/1371
CV Scoring (CVSS)	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

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_i	rt 8 1		CVE ID : CVE-2019-0901		
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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descrip	tion & CVE II	D	Pat	ch:	NCIIP	CID
			Administrato addresses thi changing how are validated. Elevation of F Vulnerability unique from CVE ID : CVE	s vulnerabi v these requ ., aka 'Wind Privilege '. This CVE CVE-2019-0	ility by uests lows ID is 0936.				
Informati on Exposure	16-05-2019	4.3	An information vulnerability Windows GD improperly dontents of it 'Windows GD Disclosure Vulnerability CVE ID is united 2019-0882, CCVE ID: CVE	exists when I componer is closes the s memory, of Information Information CVE-2019-0	n the  aka ion '. This VE-	N/A		O-MIC-V 060619	
N/A	16-05-2019	7.2	An elevation vulnerability Windows Ker handles key e 'Windows Ke Privilege Vuln CVE ID : CVE	exists when rnel impropenumeration rnel Elevat nerability'.	N/A		O-MIC-V 060619		
Informati on Exposure	16-05-2019	4.3	An information vulnerability Windows GD improperly donatents of its 'Windows GD Disclosure Vulnerability CVE ID is united 2019-0758, CCVE ID: CVE	exists when I componer is closes the s memory, of Information Information CVE-2019-0	n the  aka ion '. This VE-	N/A		O-MIC-WIND- 060619/1377	
Improper Input Validatio	16-05-2019	9.3	A remote cod vulnerability Microsoft Win properly valid	exists when	n fails to	N/A		0-MIC-V 060619	
CV Scoring (CVSS)		1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
n			aka 'Windows OLE Remote Code Execution Vulnerability'. CVE ID: CVE-2019-0885		
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1379
Improper Restrictio n of Operatio ns 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-2019-0897, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1380
Improper Restrictio n 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	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
ns within the Bounds of a Memory Buffer			memory Engine I Vulneral unique f CVE-201 0893, CV 2019-08 CVE-201 CVE-201	Remote (bility'. Tl from CVE 19-0890, 7E-2019 19-0897, 7E-2019 19-0902.	Code Execution Execution CVE-2019-0  CVE-20  CVE-20  CVE-20  -0899, C  -2019-0	ecution ID is 1989, 19- VE- 896, 19- VE- 901,				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3		oility exics Jet Dates Jet Dates Jet Dates Jet Remote Collity'. The CVF Je-2019 Je-20902.	sts when tabase E dles obje Databa Code Exe his CVE E-2019-0 -0894, C -2019-0 CVE-20 -0899, C	n the ngine cts in se ecution ID is 19-EVE-896, 19-EVE-901,	N/A		O-MIC-V 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	vulneral Window imprope memory Engine I Vulneral unique f CVE-201 0891, CV 2019-08	CVE-2019-0902.  CVE ID: CVE-2019-0893  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-2019-0899, CVE-2019-0891, CVE-2019-0893, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-					O-MIC-V 060619	
CV Scoring (CVSS		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Restrictio n of Operatio ns 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	0-MIC-WIND- 060619/1384
Improper Restrictio n of Operatio ns 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- 060619/1385
Improper Restrictio n 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
Operatio ns within the Bounds of a Memory Buffer			imprope memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0898, CV 2019-09 CVE-201	r, aka 'Jet Remote ( bility'. Tl From CVE 19-0890, /E-2019 19-0896, /E-2019 100, CVE	Databa Code Exe his CVE -2019-0 -0893, C -2019-0 CVE-20 -0899, C	se ecution ID is 0889, 19- EVE- 895, 19- EVE- 901,				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remot vulneral Window imprope memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0897, CV 2019-09 CVE-201	poility exicts Jet Date of Park Park Park Park Park Park Park Park	sts when cabase E dles object Databa Code Exe his CVE -2019-0 -0893, C -2019-0 CVE-20 -0899, C	n the ngine ects in se ecution ID is 19-EVE-19-EVE-901,	N/A		0-MIC-\ 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	CVE ID: CVE-2019-0898  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-\ 060619	
CV Scoring (CVSS)	( )- (	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	a & CVE II	)	Pat	tch	NCIIP	C ID
			CVE-203 0897, CV 2019-09 CVE-203	VE-2019 900, CVE	-0898, C -2019-0	CVE-				
			CVE ID :	<b>CVE-20</b>	19-089	9				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improper memory Engine I Vulneral unique ff CVE-2010 0891, CVE-2010 0897, CVE-2019-08 CVE-	bility exings Jet Date of Jet	sts when cabase E dles object Databa Code Exe his CVE -2019-0 -0893, C -2019-0 -0898, C -2019-0	N/A		O-MIC-\ 060619		
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902.				N/A		O-MIC-\ 060619	
Improper Restrictio	16-05-2019	9.3	A remot				N/A		0-MIC-V 060619	
CV Scoring (CVSS)	( )- (	1-2	2-3					7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
n of Operatio ns within the Bounds of a Memory Buffer			Window improper memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0897, CV 2019-08 CVE-201 CVE ID:	erly hand c, aka 'Jet Remote Coility'. The rom CVE 19-0890, 7E-2019- 19-0896, 7E-2019- 19-0901.	lles obje Databa Code Exe nis CVE -2019-0 -0893, C -2019-0 CVE-20 -0898, C	cts in se ecution ID is 19- VE-895, 19- VE-900,				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote vulneral that the Device In objects i 'GDI+ Re Vulneral CVE ID:	N/A		O-MIC-V 060619				
N/A	16-05-2019	7.2	vulnerab Window to prope symbolic Elevatio Vulneral unique f	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					O-MIC-\ 060619	
Informati on Exposure	16-05-2019	4.3	An infor vulneral Window imprope contents 'Window Disclosu	oility exists GDI coerly discless of its means were gDI In	sts wher mponer oses the emory, a lformati	n the at aka on	N/A		0-MIC-V 060619	
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	D	Pat	ch:	NCIIF	PC ID
			CVE ID is	•						
			2019-07							
. 1	2000		CVE ID :	CVE-ZU	19-096	1				
windows_s	server_2008			,			I			
Improper Input Validatio n	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 0-MIC-V 060619,			
Improper Restrictio n of Operatio ns 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-\ 060619		
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-\ 060619	
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-\ 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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		
Informati on 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
Informati on 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 Validatio n	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 Restrictio n of Operatio ns 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-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1403
Improper Restrictio n of Operatio ns 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-2019-0901, CVE-2019-0902.  CVE ID: CVE-2019-0890	N/A	O-MIC-WIND- 060619/1404

Weakness	Publish Date	cvss	·					ch	NCIIP	C ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improper memory Engine F Vulneral unique f CVE-201 0893, CVE-201 0898, CVE-201 CVE-201 CVE-201 CVE ID:	N/A		0-MIC-\ 060619				
Improper Restrictio n of Operatio ns 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-2019-0894, CVE-2019-0895, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.				N/A		0-MIC-\ 060619	
Improper Restrictio n of Operatio ns 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-\ 060619	
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

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.		
Improper Restrictio n of Operatio ns 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-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1408
Improper Restrictio n of Operatio ns 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	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			CVE ID :	CVE-20	19-089	6				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remotivulneral Window improperation of the work improvement in the work in t	N/A		O-MIC-\ 060619				
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0897, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.				N/A		O-MIC-V 060619	
Improper Restrictio n of Operatio ns 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-\ 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Descr	iption & CVE II	Pat	tch	NCIIP	C ID	
of a Memory Buffer			CVE-2019-0 0891, CVE-2 2019-0894, CVE-2019-0 0897, CVE-2	n CVE-2019-0 0890, CVE-20 2019-0893, C , CVE-2019-0 0896, CVE-20 2019-0898, C , CVE-2019-0	019- CVE- 895, 019- CVE-				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	CVE ID: CVE-2019-0899  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		0-MIC-V 060619	
Improper Restrictio n of Operatio ns 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-V 060619	
CV Scoring (CVSS)	()-	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					ch:	NCIIP	C ID
			CVE ID :	CVE-20	19-090	1				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	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-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901.				N/A		O-MIC-V 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remot vulneral that the Device I objects i 'GDI+ Re Vulnera	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-V 060619	
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-V 060619		
Informati on Exposure	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component			n the	N/A		O-MIC-V 060619	
CV Scoring (CVSS)	()-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

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_s	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	0-MIC-WIND- 060619/1419
Improper Restrictio n of Operatio ns 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

(CVSS)

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.	N/A	O-MIC-WIND- 060619/1422	
Informati on 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	0-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	
Informati on 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	
CV Scoring (CVSS)	( )- (	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish	n Date	CVSS	·				Pat	tch	NCIIP	CID
				contents 'Window Disclosu CVE ID i 2019-07	vs GDI Ir re Vulne s unique 758, CVE	nformati erability from C' -2019-0	on '. This VE- 961.				
Improper Input Validatio n	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  A remote code execution  vulnerability exists when the			N/A		0-MIC-\ 060619		
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-	2019	9.3				N/A		O-MIC-\ 060619		
Improper Restrictio n of Operatio ns 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-\ 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIPO	CID
			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 Restrictio n of Operatio ns 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-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902.	N/A		O-MIC-W 060619/	
Improper Restrictio n of Operatio ns 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-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0901, CVE-2019-0902.	N/A		O-MIC-W 060619/	
Improper	16-05-2019	9.3	A remote code execution	N/A		O-MIC-W	/IND-
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	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.			060619/1431
Improper Restrictio n of Operatio ns 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- 060619/1432
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9 9-10

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 Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1434
Improper Restrictio n of Operatio ns 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					tch	NCIIP	C ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	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-2019-0896, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.				N/A		0-MIC-\ 060619	
Improper Restrictio n of Operatio ns 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		0-MIC-\ 060619	
Improper Restrictio n of Operatio ns 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-\ 060619	
CV Scoring (CVSS)		1-2	2-3					7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	Description & CVE ID					tch	NCIIP	C ID
Memory Buffer				CVE-201 0891, CV 2019-08 CVE-201 0897, CV 2019-08 CVE-201	/E-2019 394, CVE 19-0896, /E-2019 399, CVE 19-0902.	-0893, C -2019-0 CVE-20 -0898, C -2019-0	VE- 895, 19- VE- 900,				
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901.				N/A		O-MIC-\ 060619	
Improper Restrictio n of Operatio ns 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		0-MIC-V 060619		
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		0-MIC-V 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	·					tch	NCIIP	CID
				Vulneral unique f	rom CVI	E-2019-	0734.				
Informati on Exposure	16-05	-2019	4.3	vulneral Window imprope contents 'Window Disclosu CVE ID is 2019-07	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					O-MIC-V 060619	
windows_s	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-\ 060619	
Improper Restrictio n of Operatio ns 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-\ 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Pato	h	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				
Informati on 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-W 060619/	
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		0-MIC-W 060619/	
Informati on 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		0-MIC-W 060619/	
Improper Input	16-05-2019	9.3	A remote code execution vulnerability exists when	N/A		O-MIC-W	/IND-
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Validatio			Microsoft Windows OLE fails to		060619/1452
n			properly validate user input,		
			aka 'Windows OLE Remote		
			Code Execution Vulnerability'.		
			CVE ID : CVE-2019-0885		
Informati on 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 Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1454
Improper Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0891, CVE-2019-0893, CVE-2019-0894, CVE-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.		
			CVE ID : CVE-2019-0890		
Improper Restrictio n of Operatio ns 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-2019-0897, 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 Restrictio n of Operatio ns 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

3-4

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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.		
Improper Restrictio n of Operatio ns 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-2019-0897, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1459
Improper Restrictio n of Operatio ns 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-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1460
CV Scoring (CVSS)	()-	1-2	2-3 3-4 4-5 5-6	6-7 7	7-8 8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID					tch	NCIIP	C ID
			CVE ID :	CVE-20	19-089	5				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	Window improper memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 0898, CV 2019-09 CVE-201	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-2019-0897, CVE-2019-0890, CVE-2019-0901, CVE-2019-0902.					O-MIC-\ 060619	
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0890, CVE-2019-0901, CVE-2019-0902.				N/A		O-MIC-V 060619	
Improper Restrictio n of Operatio ns within the Bounds	16-05-2019	9.3	A remote vulneral Window imprope memory Engine F	N/A		O-MIC-\ 060619				
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description	on & CVE II	D	Pat	tch	NCIIP	CID
of a Memory Buffer			unique from CV CVE-2019-089 0891, CVE-201 2019-0894, CV CVE-2019-089 0897, CVE-201 2019-0900, CV CVE-2019-090	0, CVE-20 9-0893, C E-2019-0 6, CVE-20 9-0899, C E-2019-0	19- CVE- 895, 19- CVE-				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code vulnerability ex Windows Jet Daimproperly har memory, aka 'Jo Engine Remote Vulnerability'. 'Unique from CV CVE-2019-089 0891, CVE-201 2019-0894, CV CVE-2019-089 0897, CVE-201 2019-0900, CV CVE-2019-090 CVE ID: CVE-2	N/A		O-MIC-\ 060619			
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	9.3	A remote code vulnerability ex Windows Jet Di improperly har memory, aka 'J. Engine Remote Vulnerability'. 'unique from CVCVE-2019-089 0891, CVE-201 2019-0894, CVCVE-2019-089 0897, CVE-201 2019-0899, CVCVE-2019-090	N/A		O-MIC-V 060619			
CV Scoring (CVSS)	()-	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIPC ID	
			CVE ID : CVE-2019-0900				
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0902.	O-MIC-WIND 060619/146			
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901.  CVE ID: CVE-2019-0902	N/A		O-MIC-WINE 060619/146	
Improper Restrictio n of Operatio ns 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 060619/146	
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9 9-1	0

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a			Vulnerability'.		
Memory Buffer			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
Informati on 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	D	escription	& CVE II	)	Pat	ch	NCIIP	C ID
			CVE ID :	CVE-20	19-096	1				
windows_s	server_2019						L			
N/A	16-05-2019	6.9	vulneral Network Specificandis.sys length o copying the vuln attack so could ru applicatant attacker 'Window Privilege	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					O-MIC-\ 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	16-05-2019	7.5	vulneral Window when pr crafted p DHCP Se Execution	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					O-MIC-\ 060619	
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-V 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'.		
			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'.	N/A	O-MIC-WIND- 060619/1476
			CVE ID: CVE-2019-0863		
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'.	N/A	O-MIC-WIND- 060619/1477
			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- 060619/1478
Informati on	16-05-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	0-MIC-WIND- 060619/1479
CV Scoring (CVSS)	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
Exposure			contents 'Window Disclosu CVE ID is	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						
			CVE ID:	CVE-20	19-075	8				
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'.  CVF.ID: CVF-2019-0881						O-MIC-\ 060619	
			CVE ID :	CVE ID : CVE-2019-0881						
Informati on 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-\ 060619	
Improper Input Validatio n	16-05-2019	9.3	vulneral Microso properly aka 'Win Code Exc	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					0-MIC-V 060619	
Informati on 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-\ 060619	
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'.		
			CVE ID : CVE-2019-0886		
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1484
			CVE ID : CVE-2019-0889		
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1485
Improper Restrictio n of Operatio ns 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
the 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 Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1488
Improper Restrictio n 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

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch:	NCIIP	CID
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 Restrictio n of Operatio ns 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-V 060619	
Improper Restrictio n of Operatio ns 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-V 060619	
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9	9-10

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 Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0897, CVE-2019-0900, CVE-2019-0901, CVE-2019-0902.	N/A	O-MIC-WIND- 060619/1492
Improper Restrictio n of Operatio ns 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.	N/A	O-MIC-WIND- 060619/1493
Improper Restrictio n of	16-05-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine	N/A	0-MIC-WIND- 060619/1494

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	PC ID
Operatio ns within the Bounds of a Memory Buffer			imprope memory Engine F Vulneral unique f CVE-201 0891, CV 2019-08 CVE-201 CVE-201 CVE-201							
Improper Restrictio n of Operatio ns 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		0-MIC-\ 060619	
Improper Restrictio n of Operatio ns 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-\ 060619	
CV Scoring (CVSS)	( )- (	1-2	2-3	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-2019-0896, CVE-2019- 0897, CVE-2019-0898, CVE- 2019-0899, CVE-2019-0900, CVE-2019-0902.		
			CVE ID : CVE-2019-0901		
Improper Restrictio n of Operatio ns 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-2019-0896, CVE-2019-0897, CVE-2019-0898, CVE-2019-0899, CVE-2019-0900, CVE-2019-0901.	N/A	O-MIC-WIND- 060619/1497
Improper Restrictio n of Operatio ns 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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pat	ch	NCIIP	C ID
N/A	16-05-2019	7.2	Window to prope symboli Elevatio Vulnera unique f	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					O-MIC-\ 060619	
N/A	16-05-2019	2.1	An eleval vulneral Unified of feature of improper the registry Eleval vulneral CVE ID.	N/A		O-MIC-V 060619				
Informati on 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-\ 060619	
Mitsubishi	ielectric		CVE ID :	CVE-ZU	19-090	1				
	00_firmware									
Uncontro lled Resource Consump tion	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-0 060619	•
CV Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publis	h Date	cvss	De	escription	& CVE II	D	Pat	tch	NCIIP	CID
				of-service	ce condit	ion.					
				CVE ID:	CVE-20	19-109	77				
Mobotix											
s14_firmw	are										
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- 060619	_
Motorola											
m2_firmwa	are										
Use of Externall y- Controlle d Format String	23-05	-2019	7.5	scopd or 1.01 and Use of ar Format S	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.					O-MOT- 060619	_
cx2_firmw	are										
Use of Externall y- Controlle d Format String	23-05	-2019	7.5	scopd or 1.01 and Use of ar Format S TCP por 8080.	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- 060619	
Qualcomm	Qualcomm										
qm215_fir	mware										
Integer Underflo w (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://ww w.qualcom m.com/com pany/produ		0-QUA- 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	ո & CVE II	)	Pat	tch	NCIIP	C ID
Wraparo und)			later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, in in MDM' MDM96 MSM899 Qualcon 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SI SD 820A 850, SD SDM630 Snapdra CVE ID :	ct- securi lletins E-201 2244	#_CV					
Integer Underflo w (Wrap or Wraparo und)	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:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	-
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA-QM21- 060619/1509
Improper Restrictio	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to	https://ww w.codeauro	O-QUA-QM21- 060619/1510
n of  CV Scoring (CVSS)		1-2	overwrite the existing buffer  2-3  3-4  4-5  5-6	ra.org/secu	8-9 9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE II	D	Pa	tch	NCIIP	C ID
Operatio ns within the Bounds of a Memory Buffer			which fi Snapdra Comput Connect Consum Industri Snapdra Snapdra Snapdra MDM91 MDM96 MSM890 Qualcon 212/SD SD 430, 429, SD 415, SD SD 650/ SD 845, SDM660	igon Aut e, Snapd ivity, Sn er IOT, S al IOT, S agon Mol igon Voi gon We 50, MDM 07, MDM 09W, MS 1205, SD SD 435, 450, SD 625, SD 625, SD 625, SD 625, SD 625, SD 625, SD 625, SD	o, Snapo ragon apdrago Snapdrago bile, ce & Mu arables i 49206, 49650, SM89964 SD 210/ 425, SD SD 439 615/16 632, SD 8	dragon on gon gon IoT, sic, in AU, /SD 427, /SD 636, 820A, 89,	rity- bulleti 19/04 april-2 code- aurora securi bulleti	./01/ 2019- a- ty-		
sd_600_fir	mware				-					
Integer Underflo w (Wrap or Wraparo und)	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: w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Underflo w (Wrap or Wraparo und)	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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2245	O-QUA-SD_6- 060619/1512
215_firmw	vare				

Weakness	Publish Date	cvss	Desc	ription	& CVE II	D	Pat	tch	NCIIP	C ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer over invalid hear overwrite to which fix standarago Compute, Standarago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago MDM9150, MDM9607, MSM8909V Qualcomm 212/SD 20 SD 430, SD 429, SD 45 415, SD 62 SD 650/52 SD 845 / Standarago SD 845 / Standarago Snapdrago MDM9150, MDM9607, MSM8909V Qualcomm 212/SD 20 SD 430, SD 429, SD 45 415, SD 62 SD 650/52 SD 845 / Standarago SD 650/52 SD 845 / Standarago	https:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	eauro /secu in/20 /01/ 2019-	0-QUA- 060619				
mdm9206	_firmware									
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible in happen who of elements invalid sectors later used to buffer in Srapdrago Snapdrago Snapdrago Snapdrago Snapdrago Mobile, Snain MDM920 MDM9650, MSM89966	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	O-QUA- MDM9- 060619	/1514			
CV Scoring		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Underflo w (Wrap or Wraparo und)	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 Industrial 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-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 Industrial IOT, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA- MDM9- 060619/1516
Improper Restrictio n of Operatio ns 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA- MDM9- 060619/1517

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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		
111um9607	/_firmware		D 111 1 1 1 1		
Integer Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	O-QUA- MDM9- 060619/1518

CV Scoring Scale	0-1	1_2	2-3	2-1	<b>1</b> -5	5-6	6-7	7₋0	8-9	0_10
(CVSS)	0-1	1-2	2-3	3-4	4-5	3-0	0-7	7-0	0-9	3-10

Weakness	Publish Date	CVSS	De	escription	& CVE II	Pat	ch	NCIIP	C ID					
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	invalid plater use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra	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 Industrial IOT, Snapdragon IoT, 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				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				//ww lcom l/com produ ty/bu #_CV 9-	O-QUA- MDM9- 060619	/1519
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:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- MDM9- 060619	/1520				
CV Scoring S (CVSS)	o-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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		
Improper Restrictio n of Operatio ns 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 Wearables in MDM9150, MDM9206, MDM9607, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA- MDM9- 060619/1521
			SDM660, SDX20 CVE ID : CVE-2019-2248		
mdm9650	_firmware				

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

Weakness	Publish Date	CVSS	De	escription	& CVE II	)	Pat	ch	NCIIP	C ID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 3 429, SD 615/16/632, SD 615/16/632, SD 712 / SD SD 820A 850, SD 8 SDM630 Snapdra CVE ID:	when callentary streetion lead to read gon Committed gon Committed gon IoT, Snapdrag 206, MI 205, SD 435, SD 4	culating ream information in the seam in t	g length fo from nich is nput to, y, OT, OT, agon arable ', SD 427, / SD S	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- MDM9- 060619	
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9	when cal entary stream ed to ream Snapdragon Com- gon Com- gon Com- gon Indu gon IoT, Snapdragon	culating ream mangth wh d from i agon Au apute, nectivity sumer I ssumer I Snapdra gon Voic	g length ap from lich is nput to,  OT, OT, agon ce & rables	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- MDM9- 060619	
CV Scoring S (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Wearables in MDM9150, MDM9206, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA- MDM9- 060619/1524

4-5

5-6

6-7

7-8

8-9

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restrictio n of Operatio ns 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 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA- MDM9- 060619/1525
msm8996	au_firmware				
Integer Underflo w (Wrap or Wraparo und)	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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	O-QUA- MSM8- 060619/1526
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6 482</b>	6-7 7-8	8-9 9-10

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 Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2245	O-QUA- MSM8- 060619/1527

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			Snapdra	gon_Hig	h_Med_2	2016				
			CVE ID :							
Double Free	24-05-2019	4.6	Possibility while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MDM96 MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD 5D 650/SD 670, 845 / SE SDM439 SDX20, SE CVE ID:	nning m s of smp of prope while us in Snape gon Con gon Indu gon IoT, Snapdra papdrag 9150, MI 07, MDM 50, MSM 96AU, QO nm 215, 205, SD SD 450, 625, SD 52, SD 7 SD 820A 0 850, SE 9, SDM63	ultiple 12p test er protect sing glob dragon A 1pute, sumer Ic ustrial IC Snapdra gon Voic on Wear DM9206 19640, 8909W, CS605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD 12 / SD 13, SD 835 150, SDM6	ction is cal Auto, OT, OT, agon ce & rables cables difference fine (16/SD) fine (16	https:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- MSM8- 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer of invalid he overwrith which fit is appear to connect Consum Industrith Snapdra Snapdra Snapdra	neader tr te the ex x size all gon Auto e, Snapd ivity, Sna er IOT, S al IOT, S gon Mol	ries to isting bu ocation o, Snapd ragon apdrago napdrag napdrag pile, ce & Mus	uffer in ragon n gon on IoT,	https:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- MSM8- 060619	/1529
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Dat	te CVSS	D	escription	& CVE II	)	Pa	tch	NCIIP	C ID
			MDM91 MDM96 MSM890 Qualcom 212/SD SD 430, 429, SD 415, SD SD 650/ SD 845, SDM660 CVE ID :	07, MDM 09W, MS 1m 215, 205, SD SD 435, 450, SD 625, SD 52, SD 850 7, SDX20	19650, M89964 SD 210/ 425, SD SD 439, 615/16, 632, SD 20, SD 8	SD 427, / SD /SD 636, 20A, 9,				
sd_820a_fi	rmware									
Integer Underflo w (Wrap or Wraparo und)	24-05-201	9   10	Possible happen of eleme invalid so later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, so in MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SD 820A 850, SD SDM630 Snapdra CVE ID:	when ca entary st ection le ed to rea Snapdr gon Con gon Con gon IoT, Snapdra 9206, MSM 96AU, QO nm 215, 205, SD SD 435, 450, SD 75D 415, 636, SD 710 / S 855, SD 9, SDM66 gon_Hig	lculating ream information in the length what is a gon Auricular in the length what is a gon Weat is	glength fo from hich is input to,  OT, OT, OT, agon hrable The SD S	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	O-QUA- 060619	
CV Scoring (CVSS)		1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness Publish Date	CVSS	De	escription	& CVE II	)	Pat	ch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)  24-05-2019	10	-	when callentary stracket lend to read gon Committed gon Committed gon Indugen Industry (Sonapdragen 206, MI (Sonapdragen 205, Sonapdragen 215,	culating ream mangth what from it agon Au apute, nectivity sumer Identification Wear 20M9607 (Son Wear 20M9607) (Son Wear 20M96	g length ap from ich is apput to,  y,  OT,  OT,  agon as & ables  rables  7,  SD  427,  / SD  5D  712 /  , SD  5D  850,  9,  0,	https:/w.quam.com pany/ct-securi lletins E-201 2245	com /com produ ty/bu #_CV	O-QUA- 060619	
Double Free 24-05-2019	4.6	Snapdragon_High_Med_2016  CVE ID: CVE-2019-2245  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:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	O-QUA- 060619	
CV Scoring Scale (CVSS)	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer     24-05-2019     Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer     Bounds of a Memory Buffer     24-05-2019     Since   Continue	MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, 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	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Which fix size allocation in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, 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 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20  invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon https://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & 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 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20				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		
	,	Restrictio n of Operatio ns within the Bounds of a Memory	24-05-2019	4.6	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 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	w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security-	_

Weakness I	Publish Date	CVSS	De	escription	& CVE IE	)	Pat	:ch	NCIIP	C ID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	SDM630 Snapdra	when call antary struction lead to read gon Committed gon Considering gon Industry (Sonapdrag 206, MI (Sonapdrag 206, MSM (Sonapdrag 205, Sonapdrag 205, Son	culating ream information in the land in t	s length to from hich is input to,  off,  off,	https:/w.quaim.com pany/ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	O-QUA- 060619	
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016  CVE ID: CVE-2019-2244  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				https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	_
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Industrial IOT, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA-SD_2- 060619/1536

Weakness	Publish Date	CVSS	D	escription	& CVE ID	)	Pat	tch	NCIIP	C ID
			CVE ID :	CVE-20	19-224	7				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer of invalid hoverwrith which fit Snapdra Compute Consum Industri Snapdra Snapdra Snapdra MDM91 MDM96 MSM890 Qualcom 212/SD SD 430, 429, SD 415, SD SD 650/SD 845 /SDM660 CVE ID:	neader tree the exit x size all gon Autoe, Snapd ivity, Snape IOT, Sal IOT, Sgon Mobigon Weaton, MDM 07, MDM 07, MDM 09W, MS 1205, SD 435, 450, SD 625, SD 625, SD 625, SD 850 9, SDX20	ries to isting bu ocation is o, Snapd ragon apdragoide, ce & Musarables in 19206, 19650, M8996A SD 210/6425, SD 439 /615/16/632, SD 632, SD 8, SDM43	affer in ragon n gon on IoT, ic, n SD 427, SD 636, 20A, 9,	https:/w.codera.org/rity-bulleti 19/04 april-2 code-aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619	
sd_210_fir	mware									
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	happen of eleme invalid so later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, S	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,				//ww lcom ı/com produ ty/bu #_CV 9-	0-QUA- 060619	
CV Scoring (CVSS)	( )-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2245	O-QUA-SD_2- 060619/1539

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			Snapdra	0						
			CVE ID :							
Double Free	24-05-2019	4.6	Possibility while rule instance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SE CVE ID:	nning m s of smp of prope while us in Snape gon Con gon Indu gon IoT, Snapdra papdrag 9150, MI 07, MDM 50, MSM 96AU, QO nm 215, 205, SD SD 450, 625, SD 52, SD 7 SD 820A 0 850, SE 9, SDM63	ultiple 12p test er protect sing glob dragon A 1pute, sumer Ic ustrial IC Snapdra gon Voic on Wear DM9206 19640, 8909W, CS605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD 12 / SD 13, SD 835 150, SDM6	ction is cal Auto, OT, OT, agon ce & rables cables difference fine (16/SD) fine (16	https:/w.codera.org/rity-bulleti 19/04 april-2 code-aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer o invalid h overwri which fi Snapdra Comput Connect Consum Industri Snapdra Snapdra Snapdra	ries to isting bu ocation o, Snapd ragon apdrago napdrag napdrag pile, ce & Mus	uffer in ragon n gon on IoT,	https:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619		
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	CID
ad 212 fin				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_fir	mware										
Integer Underflo w (Wrap or Wraparo und)	24-05-	-2019	10	Possible happen of eleme invalid so later used buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MDM96, MSM899, Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SD SD 820, SD 820, SD SDM630, Snapdra CVE ID:	when cantary stection lead to read to read to read to congon Congon Congon Indiger (Congon Indicate) (	lculating ream in the ength what is a gon Au inpute, nectivity sumer I ustrial IG Snapdr gon Wear SD 605, SD 210/425, SD 439, SD 625, SD 625, SD 625, SD 6450, SD 64500, SD 645000, SD 645000, SD 645000, SD 645000, SD 645000, SD 645000, SD 6450	g length fo from hich is nput ato,  y,  OT,  OT,  agon arable  y,  SD  427,  / SD  5D  5D  5D  5D  50  60  70  70  70  70  70  70  70  70  7	https:/w.quam.company/ct-securilletinsE-2012244	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness P	ublish Date	CVSS	De	escription	& CVE II	)	Pat	ch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	4-05-2019	10	Possible happen of eleme invalid plater use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Smapdra Mobile, Sin MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	https:/w.quam.com pany/ct-securi lletins E-201 2245	com /com produ ty/bu #_CV	0-QUA- 060619				
Double Free 24	4-05-2019	4.6	Possibili while ru instance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, S	https:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619				
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8999W, 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 8204, SD 835, SD 845 / SD 855, SDA660, SDM439, SDM630, SDM60, SDX20, SDX24  CVE ID : CVE-2019-2247  Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MD	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	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Which fix size allocation in Snapdragon Auto, 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 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20  https://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin  O-QUA-SD_2- 060619/1545	invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 2112/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, 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		
,		Restrictio n of Operatio ns within the Bounds of a Memory	24-05-2019	4.6	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 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	w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security-	_

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra SD 430, 50 429, SD 430, 50 615/16/632, SD	https:/w.quam.company/ct-securilletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDMS	when cal entary stream ed to ream Snapdragon Com- gon Com- gon Com- gon Indu gon IoT, Snapdragon	culating ream mangth who d from in agon Au apute, nectivity sumer I ssumer I Snapdra gon Voice on Wear	g length ap from ich is nput to, OT, OT, agon ce & cables	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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		
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 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ 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 Restrictio n of Operatio ns 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 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA-SD_4- 060619/1549
sd_425_fir	mware	1			
Integer Underflo w (Wrap or Wraparo und)	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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	O-QUA-SD_4- 060619/1550
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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 Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2245	O-QUA-SD_4- 060619/1551

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			Snapdra	0						
			CVE ID :							
Double Free	24-05-2019	4.6	Possibility while rule instance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SD SDM439 SDX20, SCVE ID:	nning m s of smp of prope while us in Snape gon Con gon Indu gon IoT, Snapdra napdrag 9150, MI 07, MDM 50, MSM 96AU, QO nm 215, 205, SD SD 450, 625, SD 52, SD 7 SD 820A 0 850, SE 9, SDM63	ultiple 12p test er protect sing glob dragon A 1pute, sumer Ic ustrial IC Snapdra gon Voic on Wear DM9206 19640, 8909W, CS605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD 12 / SD 3, SD 835 80, SDM6	ction is cal Auto, OT, OT, agon ce & cables cables f, 16/SD 636, 710 / 6, SD 0A660, 660,	https:/w.codera.org/rity-bulleti 19/04 april-2 code-aurora securi bulleti	n/20 /01/ 2019-	O-QUA- 060619	
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer of invalid he overwrith which fix Snapdra Computer Connect Consum Industrith Snapdra Snapdra Snapdra Snapdra	ries to isting bu ocation o, Snapd ragon apdrago napdrag napdrag pile, ce & Mus	uffer in ragon n gon on IoT,	https:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619		
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
sd 427 fir	mware			MDM91 MDM96 MSM890 Qualcom 212/SD SD 430, 429, SD 415, SD SD 650/ SD 845 / SDM660 CVE ID :	07, MDM 09W, MS 111111111111111111111111111111111111	19650, M89964 SD 210, 425, SD SD 439 615/16 632, SD 20, SD 8	/SD 427, /SD /SD 636, 820A,				
				Possible happen	0						
Integer Underflo w (Wrap or Wraparo und)	24-05	-2019	10	of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM96, MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra	entary streetion lead to read a Snapdragon Congon Indigon IoT, Snapdra 206, MSM 26AU, Quant 215, 205, SD 435, 450, SD 435, 450, SD 435, 50 415, 50 835, SD 835	ream in ength wid from it agon Autopute, nectivities uner I ustrial IG, Snapdr gon West B909W, CS605, SD 210/425, SD 439, SD 625, SD 625, SD 625, SD 645, SD 6	fo from hich is nput ito,  y,  OT,  OT,  agon arable  7,  / SD  427,  / SD  5 / SD  5 / SD  0M439,  10,  2016	https:/w.quam.com pany/ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	O-QUA- 060619	_
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid plater use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Smapdra Mobile, Sin MDM969 MSM899 Qualcom 212/SD SD 430, SD 430, SD 430, SD 430, SD 710 / 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	https:/w.qua.m.com pany/ct-securi lletins E-201 2245	lcom a/com produ ty/bu #_CV	0-QUA- 060619				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer or invalid hoverwrith which fix Snapdra Computer Connects Consumer Industrial Snapdra Snapdra Snapdra	ies to isting bu ocation o, Snapd ragon updrago napdrag napdrag ile, e & Mus	offer in ragon n gon on IoT,	https:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619		
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness P	ublish Date	CVSS	D	escription	1 & CVE II	)	Pat	tch	NCIIP	CID
cd 420 Symve			MDM91 MDM96 MSM890 Qualcom 212/SD SD 430, 429, SD 415, SD SD 650/ SD 845 / SDM660 CVE ID :	07, MDM 09W, MS nm 215, 205, SD SD 435, 450, SD 625, SD 52, SD 850 , SDX20	19650, M89964 SD 210/ 425, SD SD 439, 615/16, 632, SD 20, SD 8	SD 427, / SD /SD 636, 20A, 9,				
sd_429_firmw	are		<b>D</b>		, -					
Integer Underflo w (Wrap or Wraparo und)	24-05-2019		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 Industrial IOT, Snapdragon IoT, 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:/w.quam.com pany/ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	O-QUA-SD_4- 060619/1557	
CV Scoring Scale							<u> </u>			

Weakness	Publish Date	cvss	Description & CVE ID			Pa	tch	NCIIF	NCIIPC ID	
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	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://w.quam.com/pany/ct-securilletinsE-2012245	lcom n/com produ ty/bu #_CV	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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin		O-QUA-SD_4- 060619/1559		
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer     24-05-2019     Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer     Bounds of a Memory Buffer     24-05-2019     Since   Continue	MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 429, SD 430, 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	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Which fix size allocation in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, 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 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20  Inttps://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin  0-QUA-SD_4- 060619/1560	Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Memory Buffer  Improper Buffer  Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Memory Buffer  Improper Restrictio n of Operatio ns within the Buffer  Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Improper Restrictio n of Operatio n of Operatio ns within the MDM9150, MDM9206, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 435, SD 439 / SD 429, SD 435, SD 636, SD 650/52, SD 820, SD 820A, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20				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		
		Restrictio n of Operatio ns within the Bounds of a Memory	24-05-2019	4.6	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 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	w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security-	_

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	ch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 3 429, SD 615/16/632, SD 712 / SD SD 820A 850, SD 8 SDM630 Snapdra CVE ID:	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S Music, Si in MDMS	when cal entary stream ed to ream Snapdragon Com- gon Com- gon Com- gon Indu gon IoT, Snapdragon	lculating ream ma ngth wh d from in agon Au npute, nectivity sumer Io ssumer Io Snapdra gon Voic	g length ap from ich is nput to, OT, OT, agon ce & cables	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	CID
			MDM96. MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:							
Improper Restrictio n of Operatio ns 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 Wearable, 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:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	eauro /secu in/20 /01/ 2019-	0-QUA- 060619	_
sd_435_fir	mware		CVE ID :							
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	ch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16/ 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID:	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
CV Scoring So (CVSS)	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	tch	NCIIP	CID
			MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:							
Improper Restrictio n of Operatio ns 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 Wearable, 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:/w.codera.org/rity-bulleti	eauro /secu in/20 /01/ 2019-	0-QUA- 060619	_
sd_439_fir	mware			CVE-20						
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	ch	NCIIP	C ID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SE SD 820A 850, SD SDM630 Snapdra CVE ID:	https://w.qua.m.com/pany/ct-securilletins E-20122244	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM	when calentary stream to read to read gon Comgon Congon Indugon IoT, Snapdrag	lculating ream ma ngth wh d from i agon Au npute, nectivity sumer I ustrial I Snapdra gon Voic	g length ap from ich is nput to,  OT, OT, agon ce & cables	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Industrial IOT, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	0-QUA-SD_4- 060619/1569

9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restrictio n of Operatio ns 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 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	0-QUA-SD_4- 060619/1570
sd_450_fir	mware				
Integer Underflo w (Wrap or Wraparo und)	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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	O-QUA-SD_4- 060619/1571
CV Scoring (CVSS	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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 Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2245	O-QUA-SD_4- 060619/1572

Weakness	Publish Date	CVSS	Description & CVE ID					ch.	NCIIP	CID
			Snapdra	gon_Hig	h_Med_2	2016				
			CVE ID :							
Double Free	24-05-2019	4.6	Possibiliment while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96	https:/w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	O-QUA- 060619				
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	Buffer or invalid h overwrit which fir Snapdra Compute Connect Consum Industrit Snapdra Snapdra Snapdra	https:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019- a- ty- n	0-QUA- 060619	/1574			
(CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
sd_615_fir	mwaro		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		
Su_015_III	mware				<del> </del>
Integer Underflo w (Wrap or Wraparo und)	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 Industrial IOT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	0-QUA-SD_6- 060619/1575
CV Scoring (CVSS)	( )- I	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness F	Publish Date	CVSS	De	escription	& CVE IE	)	Pat	ch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	4-05-2019	10	Possible happen of eleme invalid plater use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Smapdra Mobile, Smapdra Snapdra Mobile, Smapdra Mobile, Smapdra Mobile, Smapdra Mobile, Smapdra Mobile, Smapdra Mobile, Smapdra Snapdra Snapdra Snapdra Snapdra Snapdra CVE ID:	https:/w.quam.com pany/ct-securi lletins E-201 2245	com /com produ ty/bu #_CV	0-QUA- 060619				
Double Free 2	4-05-2019	4.6	Possibili while ru instance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, S	https:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619				
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

in MDM9150, MDM9206, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 636, SD 650/52, SD 712 / SD 70, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM20, SDM20, SDM20, SDM20, SDM24  CVE ID : CVE-2019-2247  Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607,	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 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	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer  Which fix size allocation in Snapdragon Auto, 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  Intus://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	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, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD  invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Compute, Snapdragon https://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin				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		
	415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20	Restrictio n of Operatio ns within the Bounds of a Memory	24-05-2019	4.6	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 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	w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security-	_

Weakness	Publish Date	cvss	De	escription	& CVE II	D	Pat	tch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid so later used buffer in Snapdra SD 430, 429, SD 430, 429, SD 430, 429, SD 5D 430, 5D 5D 820A 850, SD 5D 820A	when callentary straction lead to read Snapdragon Congon Iota, Snapdragon Iota, Snapdragon, Snapdragon Iota, I	lculating ream information in the ength what is a gon Aumpute, nectivity sumer I was rial I (Control of the ength of the engine	g length fo from nich is nput ato,  y,  OT,  OT,  agon arable  y,  SD  427,  / SD  5D  5D  5D  5D  60  60  70  70  70  70  70  70  70  70	https:/w.quaim.com pany/ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619	_
Integer Underflo w (Wrap or Wraparo und)	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:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Industrial IOT, Snapdragon IoT, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	0-QUA-SD_6- 060619/1581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restrictio n of Operatio ns 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 Wearables in MDM9150, MDM9206, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA-SD_6- 060619/1582
sd_625_fir	mware				
Integer Underflo w (Wrap or Wraparo und)	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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	O-QUA-SD_6- 060619/1583
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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 Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2245	O-QUA-SD_6- 060619/1584

Weakness	Publish Date	CVSS	D	escription	n & CVE II	)	Pat	ch.	NCIIP	C ID
			Snapdra							
			CVE ID :							
Double Free	24-05-2019	4.6	because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MDM96 MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SE	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				//ww eauro /secu n/20 /01/ 2019- a- ty- n	O-QUA- 060619	
Improper			Buffer overflow can occur if invalid header tries to overwrite the existing buffer				https:/	•		
Restriction of operations within the Bounds of a Memory Buffer	24-05-2019	4.6	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				ra.org, rity- bulleti 19/04 april-2 code- aurora securi bulleti	/secu n/20 /01/ 2019-	0-QUA- 060619	
CV Scoring (CVSS)	( )- (	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	n & CVE II	D	Pa	tch	NCIIP	C ID
				MDM960 MSM890 Qualcom 212/SD SD 430, 429, SD 415, SD SD 650/ SD 845 / SDM660	IDM9150, MDM9206, IDM9607, MDM9650, ISM8909W, MSM8996AU, ualcomm 215, SD 210/SD 12/SD 205, SD 425, SD 427, D 430, SD 435, SD 439 / SD 29, SD 450, SD 615/16/SD 15, SD 625, SD 632, SD 636, D 650/52, SD 820, SD 820A, D 845 / SD 850, SDM439, DM660, SDX20 VE ID : CVE-2019-2248						
sd_632_fir	mware										
Integer Underflo w (Wrap or Wraparo und)	24-05	-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM MDM96, MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID:	when ca entary st ection le ed to rea Snapdr gon Con gon Con gon IoT, Snapdra 9206, MSM 96AU, QO mm 215, 205, SD SD 435, 450, SD 75D 415, 636, SD 710 / S 855, SD 9, SDM66 gon_Hig	lculating ream in a length what agon Aumpute, an activity asumer I lustrial IG, Snapdr gon West B909W, CS605, SD 210/425, SD 439, 600, SD 439, SD 625, SD 670,	g length fo from hich is hput tto,  y,  OT, OT, agon arable 7,  / SD 427, / SD 5D 820, SD 5D 820, SD 0M439, 0, 2016	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	O-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness Publ	lish Date	cvss	De	escription	& CVE II	)	Pat	ch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	5-2019	10	Possible happen of eleme invalid plater use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Smapdra Mobile, Sin MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	when call antary stracket lead to read gon Committed gon Committed gon Indugen IoT, Snapdrage 206, MI 205, SD 435, SD 450, SD 670, SD 670, SD 660, gon_Highton	culating ream mangth what from it agon Au apute, nectivity sumer Identification Wear 20M9607 (Son Wear 20M9607) (Son Wear 20M96	g length ap from ich is aput to, y, OT, OT, agon ce & rables y, SD 427, / SD 50 850, 9, 0, 2016	https:/w.quam.com pany/ct-securi lletins E-201 2245	com /com produ ty/bu #_CV	O-QUA- 060619	
Free	5-2019	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:/ w.code ra.org/ rity- bulleti 19/04 april-2 code- aurora securi bulleti	eauro /secu n/20 /01/ 2019-	0-QUA- 060619	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper   Restrictio   n of Operation   24-05-2019   Momers   M	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 240, 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, 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		
	Restrictio n of Operatio ns within the Bounds of a Memory	24-05-2019	4.6	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 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	w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security-	_
sd_636_firmware	sd_636_fir	mware				

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	ch	NCIIP	CID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID:	when callentary straction lead to read Snapdragon Congon Iota, Snapdragon Iota, Snapdragon, Snapdragon Iota, I	lculating ream information in the ength what is a gon Aumer I was trial I (Control of the ength of the engine	g length fo from nich is nput to, y, OT, OT, agon arable y, SD 427, / SD S	https://w.qua.m.com/pany/ct-securilletins E-20122244	lcom n/com produ ty/bu #_CV	0-QUA- 060619	_
Integer Underflo w (Wrap or Wraparo und)	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:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring S (CVSS)	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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 Industrial IOT, Snapdragon IoT, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	0-QUA-SD_6- 060619/1593

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2247		
Improper Restrictio n of Operatio ns 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 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	0-QUA-SD_6- 060619/1594
sd_650_fir	mware				
Integer Underflo w (Wrap or Wraparo und)	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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	0-QUA-SD_6- 060619/1595
CV Scoring (CVSS	()-	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escription	ո & CVE II	)	Pat	tch	NCIIP	C ID
			MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID :	nm 215, 205, SD SD 435, 450, SD /SD 415, 636, SD 710 / S A, SD 835 855, SDA 9, SDM66 gon_Hig	SD 210/ 425, SD SD 439, 600, SD SD 625, 650/52, 670, S A660, SD 60, SDX2 h_Med_2					
Double Free	24-05-2019	4.6	Possibility while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SCVE ID:	nning m s of smp of prope while us in Snape gon Con gon Indu gon IoT, Snapdra napdrag 9150, MI 07, MDM 50, MSM 96AU, QO nm 215, 205, SD SD 450, 625, SD 52, SD 7 SD 820A 0 850, SE 0 850, SE 0 850, SE	tultiple 2p test er protecting glob dragon A apute, sumer I ustrial IC Snapdr gon Voic OM9206 19640, 18909W, CS605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD A, SD 835 0 855, SI 30, SDM6	ction is pal Auto, OT, OT, agon ce & rables 6, 710 / 6, SD 0A660, 660,	https:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	eauro /secu in/20 /01/ 2019-	0-QUA- 060619	
Improper	24-05-2019	4.6	Buffer overflow can occur if				https:/	//ww	O-QUA-	SD_6-
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Des	scription & (	CVE ID	Pa	tch	NCIIP	C ID
Restriction of Operations within the Bounds of a Memory Buffer			overwrite which fix Snapdrag Compute, Connectiv Consume Industria Snapdrag Snapdrag Snapdrag MDM915 MDM960 MSM8909 Qualcomi 212/SD 2 SD 430, S 429, SD 4 415, SD 6 SD 650/5 SD 845 / SDM660,	, Snapdrag vity, Snapd r IOT, Snap l IOT, Snap gon Mobile, gon Voice & gon Wearal 0, MDM92 7, MDM96 9W, MSM8 m 215, SD 205, SD 425 D 435, SD 50, SD 615 25, SD 632 52, SD 820, SD 850, SD	ng buffer tion in napdragon on ragon odragon odragon IoT a Music, oles in 06, 50, 996AU, 210/SD 5, SD 427, 439 / SD 6/16/SD 2, SD 636, SD 820A, 0M439,	ra.org rity- bullet 19/0 <sup>4</sup> april- code-	ity-	060619	/1597
Integer Underflo w (Wrap or Wraparo und)	<b>mware</b> 24-05-2019	10	happen woof element invalid set later used buffer in Saparag Snapdrag Snapdrag Snapdrag Snapdrag Mobile, Strin MDM965 MSM8996	when calculatory streaments of the read from the computation of the contraction of the co	n Auto, te, etivity, ner IOT, rial IOT, apdragon Wearable 9607, 09W,	h https://w.quam.cor/pany/ct-secur	n/com /produ ity/bu s#_CV	0-QUA- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				212/SD SD 430, 429, SD 615/16, 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID :	SD 435, 450, SD /SD 415, 636, SD 0 710 / S 1, SD 835 855, SDA 1, SDM66 gon_Hig	SD 439, 600, SD SD 625, 650/52, D 670, S , SD 845 A660, SD 60, SDX2 h_Med_2	/ SD , SD SD 820, 5 / SD 0M439, 0, 2016				
Double Free	24-05-	-2019	4.6	Possibili while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SE CVE ID:	nning m s of smp of prope while us in Snape gon Con gon Indu gon IoT, Snapdrag 9150, MI 07, MDM 50, MSM 96AU, QO nm 215, SD SD 450, SD 52, SD 7 SD 820A 0 850, SD 0, SDM63 SDX24	ultiple 2p test er protecting glob dragon A pute, sumer Ic strial IC Snapdr gon Voic on Wear DM9206 19640, 8909W, CS605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD a, SD 835 160, SDM6	ction is pal Auto, OT, OT, agon ce & rables f, 16/SD 636, 710 / 6, SD 0A660, 660,	https://w.codera.org/rity-bulleti	n/20 /01/ 2019-	0-QUA- 060619	
Improper Restrictio	24-05-	-2019	4.6	Buffer or invalid h	https://ww w.codeauro		0-QUA-				
n of				overwrite the existing buffer				ra.org	/secu		-
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE II	D	Pa	tch	NCIIP	C ID
Operatio ns within the Bounds of a Memory Buffer			which fi Snapdra Comput Connect Consum Industri Snapdra Snapdra Snapdra MDM91 MDM96 MSM890 Qualcon 212/SD SD 430, 429, SD 415, SD SD 650/ SD 845, SDM660	igon Aute, Snapd ivity, Sn er IOT, S al IOT, S agon Mol igon Void gon We 50, MDM 07, MDM 09W, MS 109W,	o, Snapo ragon apdrago Snapdrago ile, ce & Mu arables i 19206, 19650, M89966 SD 210/ 425, SD SD 439 615/16 632, SD 620, SD 8	rity- bulleti 19/04 april-2 code- aurora securi bulleti	./01/ 2019- a- ty-			
sda660_fir	mware				-					
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer ir Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, in MDM MDM96 MSM899 Qualcon 212/SD SD 430,	lculating ream in a length when the control of the	https: w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619			
CV Scoring		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pa	tch	NCIIP	C ID
			632, SD 712 / SI SD 820A 850, SD SDM630 Snapdra CVE ID :	/SD 415, 636, SD 6 710 / S A, SD 835 855, SD 6, SDM66 gon_High	SD 625, 650/52, D 670, S , SD 845 A660, SD 60, SDX2 h_Med_2	SD SD 820, 5 / SD OM439, 0, 2016				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 Smapdra	ed to read a Snapdra gon Con gon Con gon Indu gon IoT, Snapdrag 9206, MI 50, MSM 96AU, QC mm 215, S 205, SD 450, SD 450, SD 636, SD 636, SD 636, SD 0 835, SI SDA660,	lculating ream mangth who defrom it agon Aumpute, nectivity sumer I ustrial IC Snapdr gon Wear DM9607, SD 210/425, SD 439, SD 625, SD 625, SD 625, SD 820, SD	g length ap from aich is input to, y, OT, OT, agon as & rables ', 'SD 427, / SD 712 / J, SD SD 850, 9, 0,	https:/w.quam.company/ct-securilletins	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
Double Free	24-05-2019	4.6	Possibility of double free issue while running multiple				https:	•	0-QUA- 060619	
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	& CVE II	)	Pa	tch	NCIIP	C ID
			because missing variable Snapdra Snapdra Snapdra Mobile, S in MDM' MDM96 MDM96 MSM899 Qualcon 212/SD SD 429, 415, SD SD 650/ SD 670, 845 / SE SDM439 SDX20, S	es of smp of prope while us in Snapo gon Con gon Indu gon IoT, Snapdrag 19150, MI 07, MDM 50, MSM 96AU, QC 196AU, QC	er protecting glob dragon A apute, sumer Id strial IG Snapdragon Void on Wear DM9206 (9640, 8909W, CS605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD 1, SD 835 0 855, SI 0, SDM6	Auto, OT, OT, agon ce & cables f, SD 439 / 16/SD 636, 710 / 6, SD 0A660, 660,	ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	in/20 ·/01/ 2019- a- ty-		
sdm439_fi	rmware									
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, in MDM9 MSM899	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2245	0-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 Industrial IOT, Snapdragon IoT, 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA-SDM4- 060619/1606
Improper Restrictio n of Operatio ns 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 Woice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA-SDM4- 060619/1607

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
adm (20 f			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_f	mmware		D 111 1 2 2		ı
Integer Underflo w (Wrap or Wraparo und)	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-2019- 2244	O-QUA-SDM6- 060619/1608

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pa	tch	NCIIF	PC ID
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	when called the react of the re	ream mangth who defrom it agon Aumer Identity sumer Identity sumer Identity sumer Identity Snapdragon Wear DM9607 8909W, SS605, SD 210/425, SD 439, SD 625, SD 625, SD 625, SD 8200 845 / SED 8200 SD	g length ap from ich is appropriately, y, OT, OT, agon as & rables /, SD 427, / SD 5D 850, 9, 0, 2016	https: w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
Double Free	24-05-2019	4.6	Possibili while ru instance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, S	nning m s of smp of prope while us in Snapo gon Com gon Con gon Indu gon IoT, Snapdra	ultiple 2p test er protec ing glob dragon A npute, sumer IC Istrial IC Snapdra gon Voice	ction is oal Auto, OT, OT, agon	https:/ w.cod/ ra.org rity- bullet/ 19/04 april-2 code- aurora securi bullet/	eauro /secu in/20 /01/ 2019-	0-QUA- 060619	
CV Scoring (CVSS	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escription	n & CVE II	D	Pat	tch	NCIIP	C ID
			in MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/ SD 670, 845 / SE SDM439 SDX20, SE CVE ID:	07, MDM 50, MSM 96AU, QO nm 215, 205, SD SD 450, 625, SD 52, SD 7 SD 820A 9 850, SE 9, SDM63	19640, 18909W, 2S605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD A, SD 835 0 855, SI 30, SDM6	/SD 439 / /16/SD 636, 710 / 5, SD DA660,				
sdm660_fi	rmware		0	0.2.2		-				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SE SD 820A 850, SD SDM630	when caentary streetion leed to read Snapdragon Congon Congon IoT, Snapdra 9206, MM 96AU, Quan 215, 205, SD 435, 450, SD 435, 450, SD 710 / SD 835, SD	lculating ream in length when the length when the length when the length when the length with the length le	g length fo from hich is nput ato,  OT, OT, agon arable 7, A27, / SD 427, / SD 5D 820, 5 / SD 0M439,	https:/w.quam.company/ct-securilletins	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
			Snapdra	gon_Hig	h_Med_2	2016				
			CVE ID:	CVE-20	19-224	4				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	when calcatary stream acket lead to read a Snapdragon Congon Indugon IoT, Snapdragon So, SD, SD, SD, SD, SD, SD, SD, SD, SD, SD	lculating ream mangth who defrom it agon Aumpute, nectivity sumer Idustrial ICustrial	g length ap from ich is aput to, y, OT, OT, agon ce & cables y, SD 427, / SD 50 850, 9, 0, 2016	https:/w.qualm.com pany/ct- securilletins E-201 2245	lcom n/com produ ty/bu #_CV	O-QUA- 060619	
			Possibili	_		issue	https:/	•		
Double Free	24-05-2019	4.6	while ru instance because missing variable Snapdra Snapdra Snapdra	s of smp of prope while us in Snape gon Con gon Con	2p test er protecting glob dragon A pute, sumer I	al Auto, OT,	w.code ra.org, rity- bulleti 19/04 april-2 code- aurora	/secu n/20 /01/ 2019-	0-QUA- 060619	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	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 Restrictio n of Operatio ns 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 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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019- code- aurora- security- bulletin	O-QUA-SDM6- 060619/1614

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
			CVE ID : CVE-2019-2248							
snapdrago	n_high_med_2	2016_fi	rmware							
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid so later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MDM96, MSM899, Qualcom 212/SD SD 430, 429, SD 615/16/632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID:	when caentary streetion lead to read to read a Snapdragon Confegon Confegon IoT, Snapdragon Io	lculating ream information in the length what is a gon Auropute, nectivity sumer I sustrial IC Snapdres of SD 999W, CS605, SD 210/425, SD 439, SD 625, SD 625, SD 625, SD 6450, SD 64500, SD 645000, SD 645000	g length fo from hich is input to,  y,  OT,  OT,  agon arable  /,  / SD  427,  / SD  5D  5D  5D  5D  5D  60  70  70  70  70  70  70  70  70  70	https:/w.quam.com pany/ct-securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
Integer Underflo w (Wrap or Wraparo und)	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:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Descrip	otion & CVE II	D	Pat	tch	NCIIP	CID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05-2019	4.6	SD 670, SD 8 845 / SD 850 SDM439, SDI SDX20, SDX2 CVE ID : CVE Buffer overflinvalid header overwrite the which fix size Snapdragon Compute, Snapdragon Connectivity, Consumer IO Industrial IO Snapdragon Snapdragon Snapdragon Snapdragon MDM9150, MMM8909W, Qualcomm 2 212/SD 205, SD 430, SD 4 429, SD 450, 415, SD 625, SD 650/52, SD 845 / SD SDM660, SD	20A, SD 835, SI M630, SDM64  2-2019-224 ow can occurrence tries to e existing be allocation Auto, Snapdragor, Snap	5, SD DA660, 660, 7 ur if uffer in dragon on IoT, sic, n AU, SD 427, / SD 636, 320A, 39,	https:/w.codera.org/rity-bulletiapril-2code-aurorasecuribulleti	//ww eauro /secu in/20 /01/ 2019-	0-QUA- MDM9- 060619	
mdm9640	_firmware								
Double Free	24-05-2019	4.6	Possibility of while runnin instances of sibecause of promissing while variable in Strandragon Snapdragon Snapdragon Snapdragon Snapdragon	https:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi	eauro /secu in/20 /01/ 2019-	O-QUA- MDM9- 060619			
CV Scoring (CVSS)	( )- (	1-2	2-3 3-4	4 4-5	5-6	6-7	7-8	8-9	9-10

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	
msm8909	w_firmware				
Integer Underflo w (Wrap or Wraparo und)	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 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-
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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  Possible integer underflow can happen when calculating length		
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	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 Industrial IOT, Snapdragon IoT, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins#_CV E-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://ww w.codeauro ra.org/secu rity- bulletin/20 19/04/01/ april-2019-	O-QUA- MSM8- 060619/1622
CV Scoring (CVSS)	()-	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	Pa	tch	NCIIP	CID	
			Snapdra Snapdra Snapdra Mobile, S Music, Si in MDM9 MDM969 MDM969 Qualcom 212/SD SD 429, 3 415, SD SD 650/ SD 670, 3 SD 670, 3 SD 429, 5 CVE ID :	gon Indugon IoT, Snapdragon 105, MI 9150, MI 97, MDM 50, MSM 96AU, QC 100, SD 100, SD	strial IG Snapdr gon Voic on Wear DM9206 19640, 8909W, SS605, SD 210/ 425, SD 5D 615/ 632, SD 12 / SD , SD 835 855, SI 0, SDM6	code- aurora securi bullet	ty-			
Improper Restrictio n of Operatio ns 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 Wearables in MDM9150, MDM9206, MDM9607, 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,				https: w.cod ra.org rity- bullet 19/04 april-2 code- aurora securi bullet	eauro /secu in/20 ·/01/ 2019- a- ty-	O-QUA- MSM8- 060619	
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	Pat	tch	NCIIP	CID	
			SDM660	, SDX20						
			CVE ID :	CVE-20	19-224	8				
qcs605_fir	mware									
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 430, 429, SD 615/16/632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID:	when calcentary streetion lead to read Snapdragon Congon IoT, Snapdragon JoT, Snapdragon JoT, Snapdragon JoT, Snapdragon JoT, SD 435, SD 450, SD 835, SD 466, SD 6710 / SD 835, SD 666, SD 6710 / SD 855, SD 675, SD 6	lculating ream information in the langth what is a gon Aurigumer Instrial IC Snapdr gon West Shapper S	g length fo from hich is hput tto,  y,  OT,  OT, agon arable y,  SD 427, / SD 5D 820, SD SD 820, SD 9M439, 0, 2016 4	https:/w.quam.company/ct-securilletinsE-2012244	lcom n/com produ ty/bu #_CV 9-	O-QUA- 060619	_
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	-			
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pa	tch	NCIIP	CID
			Snapdra Mobile, S Music, Si in MDM9 MDM969 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16/ 632, SD SD 710 / 820A, SI SD 855, SDM630 SM7150 Snapdra	Snapdrag napdrag 9206, MI 50, MSM 96AU, QO nm 215, 3 205, SD 450, SD 450, SD 7 SD 415, 636, SD 9 835, SI SDA660, 1, SDM66	gon Voic on Wear 0M9607 8909W, CS605, SD 210/ 425, SD SD 439, 600, SD SD 625, 5D 820 0 845 / S , SDM43					
Double Free	24-05-2019	4.6	Possibility while run instance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 20 670, 2	ty of dou nning m s of smp of prope while us in Snape gon Con gon IoT, Snapdrag 150, MI 07, MDM 50, MSM 26AU, QC am 215, S 205, SD SD 450, S 52, SD 7	uble free ultiple 2p test er protecting glob dragon A apute, sumer I ustrial IG Snapdr gon Voic on Wear DM9206 19640, 8909W, CS605, SD 210/ 425, SD SD 615/ 632, SD	e issue ction is cal Auto, OT, OT, agon ce & rables c, 16/SD 636, 710 /	https:/ w.cod/ ra.org rity- bullet/ 19/04 april-2 code- aurora securi bullet/	eauro /secu in/20 ·/01/ 2019- a- ty-	0-QUA- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2247  Kernel can write to arbitrary	
Kernel can write to arbitrary	
1 /4-05-7019 1/7   a	QCS6- 9/1627
CVE ID : CVE-2019-2250	
sd_670_firmware	
or Wraparo und)  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	-SD_6- 9/1628
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	9-10

Weakness	Publish	Date	CVSS	De	escription	& CVE II	)	Pat	ch	NCIIP	C ID
				850, SD SDM630 Snapdra CVE ID:	, SDM66 gon_Hig CVE-20	0, SDX2 h_Med_2 <b>19-224</b>					
Integer Underflo w (Wrap or Wraparo und)	24-05-2	2019	10	Possible happen of eleme invalid plater use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	when calculated to react the calculation of the calculated to react the calcul	lculating ream mangth who differs from it agon Authorities, nectivity, sumer Identification Weard DM9607, SD 425, SD 439, SD 625, SD 625, SD 625, SD 820, SD 8	g length ap from aich is ap from aich is ap from aich is ap from ach is approximate to, by, OT, OT, agon agon agon agon agon agon agon agon	https://w.qualm.company/ct-securilletins E-201 2245	com /com produ ty/bu #_CV	O-QUA- 060619	
Double Free	24-05-2	2019	4.6	Possibili while ru instance because missing variable Snapdra	nning m s of smp of prope while us in Snape	ultiple 2p test er protec ing glob dragon A	ction is oal	https:/ w.code ra.org rity- bulleti 19/04 april-2	eauro /secu n/20 /01/	0-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Do	escription	& CVE II	)	Pat	tch	NCIIP	CID
			Snapdra Snapdra Snapdra Mobile, S Music, Si in MDM96 MDM966 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/ SD 670, 845 / SE SDM439 SDX20, S	code- aurora securi bulleti	ty-					
Improper Input Validatio n	24-05-2019	7.2	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,				https:/ w.qua m.com pany/ ct- securi lletins E-201 2250	lcom n/com produ ty/bu #_CV	0-QUA- 060619	_
sd_675_fir	mware									
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra	https://w.qua.m.com/pany/ct-securilletins	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	a & CVE II	)	Pat	tch	NCIIP	C ID
				Snapdra Snapdra Snapdra Mobile, S Music, S in MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	gon Indugon IoT, Snapdrag 1206, MI 50, MSM 16AU, QO 1m 215, 1205, SD 435, SD 450, SD 450, SD 636, SD 7 SD 4660, The SDM66	ustrial IG Snapdr gon Voic on Wear DM9607 8909W, CS605, SD 210/ 425, SD SD 439, 600, SD SD 625, 5D 825, 5D 825, 5D 845 / S , SDM43 60, SDX2 h_Med_2	OT, agon ce & rables rables r, SD 427, SD 712 / SD SD 850, 9, 0,	2245			
Improper Input Validatio n	24-05	-2019	7.2	Kernel c memory user whi thread in Snapdra Snapdra SD 675, 670, SD SD 855, SXR1130 CVE ID:	https:/ w.qua m.com pany/ ct- securi lletins E-201 2250	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
sd_710_fir	mware	1									
Integer Underflo w (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,					//ww lcom n/com produ ty/bu	0-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
und)			Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 6 615/16, 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID :	gon Con gon Con gon Indu gon IoT, Snapdrag 9206, MI 50, MSM 96AU, QO nm 215, S 205, SD SD 435, S 450, SD (SD 415, 636, SD 636, SD 636, SD 635, SD 635, SD 636, SD 636, SD 636, SD 636, SD	nectivity sumer I strial IG Snapdr gon Wea DM9607 8909W, CS605, SD 210/ 425, SD SD 439, SD 625, 650/52, D 670, SD , SD 845 0, SDX2 h_Med_2	OT, OT, agon arable ', SD 427, / SD SD 820, S / SD OM439, 0,	lletins E-201 2244	_		
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 429, SD	when calculated to react to re	lculating ream mangth who defrom it agon Aumer Instrial IC Snapdr gon Voice on Weard DM96078909W, CS605, SD 210/425, SD 439, S	g length ap from aich is input to,  OT, OT, agon ce & rables  7,  SD 427,	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	O-QUA- 060619	_
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish	n Date	CVSS	De	escription	n & CVE II	)	Pat	tch	NCIIP	C ID
				615/16/ 632, SD SD 710 / 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID :	636, SD / SD 670 D 835, SI SDA660, , SDM66 , gon_Hig CVE-20	675, SD , SD 820 ) 845 / S , SDM43 50, SDX2 h_Med_2	712 / 7, SD SD 850, 9, 0, 2016				
Double	24-05-2	2019	4.6	Possibility while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM966 MDM966 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SD SDM439 SDX20, SCVE ID:	ction is bal Auto, OT, OT, agon ce & rables 5, (16/SD 636, 710 / 5, SD 0A660,	https:/w.codera.org/rity-bulleti 19/04 april-2 code-aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619			
Improper Input Validatio n	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,					//ww lcom ı/com produ	0-QUA- 060619	_
CV Scoring (CVSS)		0-1	1-2	2-3	5-6	6-7	7-8	8-9	9-10		

Weakness	Publis	h Date	CVSS	D	escription	ı & CVE II	D	Pat	tch	NCIIP	CID
				Snapdra Snapdra SD 675, 670, SD SD 855, SXR1130	gon Mol SD 712 , 835, SD SD 8CX,	oile in Q / SD 710 845 / SI	CS605, ) / SD ) 850,	securi lletins E-201 2250	#_CV		
				CVE ID:	CVE-20	19-225	0				
sd_712_fir	mware	:									
Integer Underflo w (Wrap or Wraparo und)	24-05	-2019	10	Possible happen of eleme invalid so later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16/632, SD 712 / SE SD 820A 850, SD SDM630 Snapdra CVE ID:	when ca entary st ection le ed to rea snapdr gon Con gon Con gon IoT, Snapdra 9206, MSM 96AU, QO mm 215, 205, SD SD 435, 450, SD /SD 415, 636, SD 0 710 / S a, SD 835 855, SDA 9, SDM66 gon_Hig	lculating ream integrated with a from it agon Autopute, nectivity sumer I ustrial IG Snapdr gon West Shapper SD 439 (SD 439 (SD 439 (SD 625 (SD 670, SD 670, S	g length fo from hich is hput tto,  y,  OT,  OT, agon arable y,  SD 427, / SD 5D 820, SD SD 820, SO 9016 4	https://w.quam.company/ct-securilletins	lcom a/com produ ty/bu #_CV 9-	0-QUA- 060619	
Integer Underflo w (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					//ww lcom ı/com produ	0-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2						7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	ո & CVE II	D	Pat	tch	NCIIP	C ID
und)			buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM' MDM96 MSM899 Qualcon 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra	igon Con igon Con igon Con igon Indi igon IoT, Snapdra napdrag 9206, MS 96AU, Qo nm 215, 205, SD SD 435, 450, SD /SD 415, 636, SD /SD 670 D 835, SI SDA660 D, SDM66	npute, inectivity isumer I ustrial IG , Snapdr gon Void gon Wear DM9607 (8909W) CS605, SD 210/ 425, SD SD 439, 600, SD , SD 625 675, SD 9, SD 820 D 845 / S 1, SDM43 60, SDX2	y, OT, OT, agon ce & rables r, /SD 427, /SD 5D 850, 9, 0,	securi lletins E-201 2245	#_CV		
Double Free	24-05-2019	4.6	Possibility while rule instance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MDM96 MDM96 MSM899 Qualcon	es of smp of propo while us in Snap gon Con gon Ind gon IoT, Snapdra napdrag 9150, M 07, MDM 50, MSM	er protesting glob dragon Anpute, sumer I ustrial IG, Snapdr gon Voice OM9206 19640, 18909W,	ction is oal Auto, OT, OT, agon ce & rables	https:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619	_
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Da	ate	CVSS	De	escription	& CVE II	)	Pa	tch	NCIIP	C ID
				212/SD SD 429, 415, SD SD 650/ SD 670, 845 / SD SDM439 SDX20, S	SD 450, 3 625, SD 6 52, SD 7 SD 820A 0 850, SD 0, SDM63	SD 615/ 632, SD 12 / SD ,, SD 835 ) 855, SI	16/SD 636, 710 / 5, SD DA660,				
				CVE ID:	CVE-20	19-224	7				
Improper Input Validatio n	24-05-20	19	7.2	Kernel comemory user whithread in Snapdra Snapdra SD 675, 2670, SD 855, 25XR1130	https:/ w.qua m.com pany/ ct- securi lletins E-201 2250	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
sd_820_fir	mware										
Integer Underflo w (Wrap or Wraparo und)	24-05-20	19	10	Possible happen of eleme invalid s later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MDM965 MSM899 Qualcom 212/SD SD 430, 5	when callentary streetion lead to read to read some congon Congon Congon Indugon IoT, Snapdrag 9206, MI 50, MSM 96AU, QC am 215, SD 205, SD	lculating ream information in the second in	g length To from nich is nput to, OT, OT, agon nrable t,	https: w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	O-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	SD 430, SD 435, SD 439 / SD  2-3 3-4 4-5 5-6					7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pa	tch	NCIIP	C ID
			SD 820A 850, SD SDM630 Snapdra	/SD 415, 636, SD 6 710 / S A, SD 835 855, SD 6, SDM66 gon_Hig	SD 625, 650/52, D 670, S , SD 845 A660, SD 60, SDX2 h_Med_2	SD SD 820, 5 / SD OM439, 0, 2016				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM <sup>o</sup> MDM96 MSM899	when callentary stroacket lead to read a Snapdragon Congon Indugon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, South IoT, South IoT, South IoT, IoT, IoT, IoT, IoT, IoT, IoT, IoT,	lculating ream mangth who defrom it agon Authorities, nectivity, sumer I ustrial IC Snapdres on Weard DM9607, SD 210/425, SD 439, SD 625, SD 625, SD 625, SD 820, SD 8	g length ap from aich is input to, y, OT, OT, agon as & rables ', 'SD 427, / SD 712 / J, SD SD 850, 9, 0,	https://w.quam.com/pany/ct-securilletins	lcom n/com produ ty/bu #_CV	0-QUA- 060619	/1643
Improper Restrictio	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to					//ww eauro	0-QUA- 060619	
CV Scoring (CVSS)	( ) - (	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	D	Pa	tch	NCIIP	C ID
n of Operatio ns within the Bounds of a Memory Buffer			overwri which fi Snapdra Comput Connect Consum Industri Snapdra Snapdra MDM91 MDM96 MSM890 Qualcon 212/SD SD 430, 429, SD 415, SD SD 650/ SD 845, SDM660	x size allagon Aute, Snapdivity, Snapdivity, Snapdivity, Snapon Word, MDM, Son West, Son MDM, MS, Son West, Son West	location o, Snapo ragon apdrago Snapdrago inapdrago ile, ce & Mu arables i 19206, 19650, SM89966 SD 210/ 425, SD SD 439 615/16 632, SD 620, SD 8	in Iragon Iragon gon IoT, sic, n AU, /SD 427, /SD 636, 820A,	ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	in/20 ·/01/ 2019- a- ty-		
sd_835_fir	mware									
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid so later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, in MDM MDM96 MSM899 Qualcon 212/SD	when ca entary st section le ed to rea a Snapdr agon Con agon Con agon Inda gon Inda gon Inda gon IoT, Snapdra 9206, M 50, MSM 96AU, Qo	lculating ream in ength what d from it agon Au npute, inectivity isumer I ustrial IG Snapdr gon West BM9607 (8909W) (SS605, SD 210/	g length fo from hich is nput tto,  OT, OT, agon arable 7,	https:/ w.qua m.com pany/ ct- securi lletins E-201 2244	lcom n/com produ ty/bu #_CV	0-QUA- 060619	_
CV Scoring		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	D	escription	a & CVE II	)	Pa	tch	NCIIP	CID
			SD 430, 429, SD 615/16, 632, SD 712 / SI SD 820, 850, SD SDM630 Snapdra CVE ID :	450, SD (/SD 415, 636, SD (/SD 835, SD 855, SD 66, SD M66, gon_Hig.	600, SD SD 625, 650/52, D 670, S S, SD 845, A660, SD SO, SDX2 h_Med_2	, SD SD 820, 5 / SD 0M439, 0, 2016				
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	happen of eleme invalid plater use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	when calentary streat to read to read son Comercial gon Comercial gon Comercial gon IoT, Snapdrag 19206, MI 19205, SD 435, SD 436, SD	lculating ream mangth who defrom it agon Authorities, nectivity, sumer I ustrial IG Snapdr gon Wear DM9607, SD 439, SD 439, SD 600, SD 675, SD 600, SD 675, SD 820, SD	g length ap from aich is input ito,  y,  OT,  OT,  agon as a sea sea sea sea sea sea sea sea se	https: w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu t#_CV	0-QUA- 060619	_
Double	24-05-2019	4.6	Possibili	https:	//ww	O-QUA-	SD_8-			
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	)	Pat	tch	NCIIP	CID
Free			while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MDM96 MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SE CVE ID:	es of smp of prope while us in Snape gon Con gon IoT, Snapdrag 9150, MI 07, MDM 50, MSM 96AU, QO mm 215, SD 205, SD SD 450, SD 52, SD 7 SD 820A 0 850, SD 0, SDM63 SDX24	2p test er protecting glob dragon Apute, sumer I ustrial IC Snapdr gon Voice OM 9206 (19640, 18909W, 1890W, 18	Auto, OT, OT, agon ce & rables 6, (16/SD 636, 710 / 6, SD 0A660, 660,	w.codera.org	/secu in/20 /01/ 2019- a- ty-	060619	/1647
Improper Input Validatio n	24-05-2019	7.2	Kernel c memory user whi thread in Snapdra Snapdra Snapdra SD 675, 670, SD SD 855, SXR1130	r address ile freein n Snapdr gon Con gon Indu gon Mob SD 712 / 835, SD 8 SD 8CX, 8	s passed ng/stopp ragon Co sumer I ustrial IO pile in Qo / SD 710 845 / SI SM7150	by oing a ompute, OT, OT, CS605, O / SD O 850,	https:/ w.qua m.com pany/ ct- securi lletins E-201 2250	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
sd_845_fir	mware		Donailala		d (1		1.44	1.1		
Integer Underflo	24-05-2019	10	Possible happen	_			https:/ w.qua	•	O-QUA-	SD_8-
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
w (Wrap or Wraparo und)			of elementary invalid solution in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 430, 429, SD 615/16/632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID:	ection lead to read son Commigon Commigon IoT, Snapdrag 206, MI 205, SD 435, SD 450, S	ength when d from it agon Au apute, nectivity sumer IC snapdragon Weaton SD 439 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 52 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 / 650 /	nich is nput to, y, OT, OT, agon arable y, SD 427, / SD S	m.com pany/ ct- securi lletins E-201 2244	produ ty/bu #_CV	060619	/1649
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899	when cal entary stream ed to ream Snapdragon Con- gon Con- gon Indu gon IoT, Snapdragon 9206, MI	lculating ream ma ngth wh d from it agon Au npute, nectivity sumer IO Snapdra gon Voic on Wear OM9607 8909W,	g length ap from ich is nput to, OT, OT, agon ce & cables	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	n & CVE II	)	Pa	tch	NCIIP	C ID
			Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra	205, SD SD 435, 450, SD /SD 415, 636, SD / SD 670 D 835, SI SDA660, J, SDM66	425, SD SD 439, 600, SD SD 625, 675, SD , SD 820 D 845 / S , SDM43 60, SDX2 h_Med_2	427, / SD , SD 712 / , SD SD 850, 9, 0,				
Double	24-05-2019	4.6	Possibility while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SCVE ID:	ity of dou nning mes of smp of prope while us in Snape gon Con gon IoT, Snapdrag 9150, MI 07, MDM 50, MSM 96AU, QO mm 215, SD SD 450, SD SD 450, SD SD 820A 0 850, SD 0 850, SD	uble free cultiple of the protect of	e issue ction is cal Auto, OT, OT, agon ce & rables 6, 716/SD 636, 710 / 6, SD 0A660, 660,	https:; w.cod ra.org rity- bullet: 19/04 april-2 code- aurora securi bullet:	eauro /secu in/20 /01/ 2019-	0-QUA- 060619	
Improper	24-05-2019	4.6	Buffer overflow can occur if					//ww	O-QUA-	SD_8-
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	D	Pat	tch	NCIIP	CID
Restrictio n of Operatio ns within the Bounds of a Memory Buffer			invalid h overwrit which fix Snapdra Compute Connecti Consume Industria Snapdra Snapdra Snapdra MDM915 MDM960 MSM890 Qualcom 212/SD 2 429, SD 4 415, SD 6 SD 650/SD 845 / SDM660 CVE ID:	te the exite size allows size allows a size	isting brocation of Snapdragon apdragon apdragon apdragonile, arables in 19206, 19650, 19650, SD 439, 19615/16, 1920, SD 439, SDM43	in Iragon n gon gon IoT, sic, n AU, 'SD 427, /SD 636, 820A,	w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	/secu n/20 /01/ 2019- a- ty-	060619	/1652
Improper Input Validatio n	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				https:/ w.qua m.com pany/ ct- securi lletins E-201 2250	lcom a/com produ ty/bu #_CV	0-QUA- 060619	
ad 050 6			CVE ID :	CVE-20	19-225	0				
sd_850_fir	mware		Doggible	integer	undonfl	OTAL 622	https:	//*****		
Integer Underflo w (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:/ w.qua m.com pany/	lcom 1/com	0-QUA- 060619	
CV Scoring (CVSS)	()-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	ո & CVE II	)	Pat	tch	NCIIP	C ID
Wraparo und)			later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, in in MDM' MDM96 MSM899 Qualcon 212/SD SD 430, 429, SD 615/16, 632, SD 712 / SI SD 820A 850, SD SDM630 Snapdra CVE ID :	a Snapdragon Congon Congon Congon Indiagon IoT, Snapdra 9206, MSM 215, 205, SD 435, 450, SD 415, 636, SD 710 / S 855, SDM66 agon_Hig	agon Au npute, nectivity sumer I ustrial IG Snapdr gon Wea DM9607 8909W, CS605, SD 210/ 425, SD SD 439, 600, SD 650/52, GD 670, S GA660, SE A660, SE	to, y, OT, OT, agon arable y, SD 427, / SD S	ct- securi lletins E-201 2244	#_CV		
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Mobile, Music, S in MDM MDM96 MSM899 Qualcon 212/SD	https:/w.quam.com pany/ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619				
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE II	D	Pat	tch	NCIIF	PC ID
			429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra	SD 435, 9 450, SD 6 /SD 415, 636, SD 6 / SD 670, D 835, SD SDA660, D, SDM66 , gon_High	500, SD SD 625, 575, SD SD 820 845 / S SDM43 0, SDX2	, SD 712 / ), SD SD 850, 9, 0,				
Double Free	24-05-2019	4.6	while ruinstance because missing variable Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM MDM96 MDM96 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SE SDX20	of prope while us in Snapo gon Com gon Indu gon IoT, Snapdrag 9150, MI 07, MDM 50, MSM 96AU, QC 1m 215, S 205, SD 52, SD 6 52, SD 7 SD 820A 0, SDM63	ultiple 2p test 2p test 2p test 2p test 2p test 3r protec 3r glob 4ragon A 2pute, 2sumer Ic 2snapdr 20M9206 29640, 8909W, 25605, 250 615/ 632, SD 425, SD 12 / SD 455, SI 0, SDM6	ction is pal Auto, OT, OT, agon ce & rables 6, 710 / 6, SD 0A660, 660,	https://w.codera.org/rity-bulleti/2code-aurorasecuri/bulleti/	eauro /secu in/20 /01/ 2019-	O-QUA- 060619	_
Improper Restrictio	24-05-2019	4.6	Buffer overflow can occur if invalid header tries to					//ww eauro	0-QUA- 060619	
n of			overwri	te the ex	isting bu	uffer	ra.org	/secu	000019	7/103/
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	ı & CVE II	D	Pat	tch	NCIIP	C ID
Operatio ns within the Bounds of a Memory Buffer				which fix Snapdra Compute Connect Consum Industria Snapdra Snapdra Snapdra MDM96 MSM890 Qualcom 212/SD SD 430, 429, SD 415, SD SD 650/SD 845 /SDM660 CVE ID:	gon Auto e, Snapd ivity, Sna er IOT, S al IOT, S gon Mob gon Voic gon Wea 50, MDM 07, MDM 09W, MS nm 215, S 205, SD SD 435, S 450, SD 625, SD 625, SD 625, SD 7, SD 850 7, SDX20 CVE-20	o, Snapdragon apdragon apdragon apdragon apdragon bile, arables in 19206, 19650, M89964 SD 210/425, SD 439, 615/16, 632, SD 80, SD 439, SD 439	lragon  n gon gon IoT, sic, n AU, SD 427, / SD /SD 636, 820A, 89,	rity- bulleti 19/04 april-2 code- aurora securi bulleti	/01/ 2019- a- ty-		
Improper Input Validatio n	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:/ w.qua m.com pany/ ct- securi lletins E-201 2250	lcom n/com produ ty/bu #_CV	O-QUA- 060619	
sd_855_fir	mware	!									
Integer Underflo w (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://w.quam.com/pany/ct-securi	lcom ı/com produ	0-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	CID
und)			Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 6 615/16, 632, SD 712 / SD SD 820A 850, SD SDM630 Snapdra CVE ID :	gon Con gon Con gon Indu gon IoT, Snapdrag 9206, MI 50, MSM 96AU, QO nm 215, S 205, SD SD 435, S 450, SD (SD 415, 636, SD 636, SD 636, SD 635, SD 635, SD 636, SD 636, SD 636, SD 636, SD	nectivity sumer I sumer I Snapdr gon Wea DM9607 8909W, CS605, SD 210/ 425, SD SD 439, SD 625, 650/52, D 670, SD , SD 845 0, SDX2 h_Med_2	OT, OT, agon arable ', SD 427, / SD SD 820, S / SD OM439, 0,	lletins E-201 2244	_		
Integer Underflo w (Wrap or Wraparo und)	24-05-2019	10	Possible happen of eleme invalid p later use buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM9 MSM899 Qualcom 212/SD SD 430, 429, SD	when calculated to react to re	lculating ream mangth who defrom it agon Aumer Instrial IC Snapdr gon Voice on Weard DM96078909W, CS605, SD 210/425, SD 439, S	g length ap from aich is apput to, y, OT, OT, agon ce & rables ', SD 427,	https:/ w.qua m.com pany/ ct- securi lletins E-201 2245	lcom n/com produ ty/bu #_CV	0-QUA- 060619	_
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish	n Date	cvss	De	escription	a & CVE II	)	Pat	tch	NCIIP	C ID
				615/16/ 632, SD SD 710 / 820A, SI SD 855, SDM630 SM7150 Snapdra	636, SD 7 SD 670 0 835, SI SDA660, 1, SDM66 1, gon_Hig CVE-20	675, SD , SD 820 ) 845 / S , SDM43 60, SDX2 h_Med_2	712 / , SD SD 850, 9, 0, 2016				
Double Free	24-05-	2019	4.6	Possibility while rule instance because missing variable Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Sin MDM966 MDM966 MSM899 Qualcom 212/SD SD 429, 415, SD SD 650/SD 670, 845 / SE SDM439 SDX20, SCVE ID:	nning m s of smp of prope while us in Snape gon Con gon Indu gon IoT, Snapdrag 9150, MI 07, MDM 50, MSM 96AU, QO am 215, SD 52, SD 52, SD 52, SD 7 SD 820A 9850, SD 50, SD 850, SD 50, SD	ultiple 2p test er protecting glob dragon A pute, sumer I ustrial IC Snapdr gon Voic on Wear DM9206 19640, 8909W, CS605, SD 210/ 425, SD SD 615/ 632, SD 12 / SD 12 / SD 3, SD 835 0 855, SI 80, SDM6	ction is bal Auto, OT, OT, agon ce & rables 5, (16/SD 636, 710 / 5, SD 0A660,	https://w.codera.org/rity-bulleti/april-2code-aurorasecuri/bulleti/	eauro /secu in/20 /01/ 2019-	0-QUA- 060619	
Improper Input Validatio n	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:/ w.qua m.com pany/ ct-	lcom 1/com	0-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	D	escription	a & CVE II	D	Pat	:ch	NCIIP	CID
				Snapdra Snapdra SD 675, 670, SD SD 855, SXR1130	gon Mol SD 712 , 835, SD SD 8CX,	oile in Q / SD 710 845 / SI	CS605, ) / SD ) 850,	securi lletins E-201 2250	#_CV		
				CVE ID:	CVE-20	19-225	0				
sdx20_firm	nware										
Integer Underflo w (Wrap or Wraparo und)	24-05	-2019	10	Possible happen of eleme invalid stater use buffer in Snapdra SD 430, 429, SD 430, 429, SD 615/16/632, SD 712 / SD 820A 850, SD SDM630 Snapdra CVE ID:	when ca entary st ection le ed to rea snapdr gon Con gon Con gon IoT, Snapdra 9206, MSM 96AU, QO mm 215, 205, SD SD 435, 450, SD /SD 415, 636, SD 0 710 / So 1, SD 835 9, SDM66 gon_Hig CVE-20	lculating ream integrated with a from it agon Autopute, nectivity sumer I ustrial IG Snapdr gon Wear Shapper SD 439, SD 439, SD 439, SD 625, SD 625, SD 625, SD 6450, SD 6450, SD 8450, SD 84500, SD 845000, SD 8450000, SD 845000000000000000000000000000000000000	g length fo from hich is hput tto,  y,  OT,  OT, agon arable y,  SD 427, / SD 5 D 5 SD 5 D 5 SD 5 O 6 SD	https://w.quam.company/ct-securilletins	lcom l/com produ ty/bu #_CV 9-	0-QUA- 060619	
Integer Underflo w (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				_		0-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
und)			buffer in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16/ 632, SD SD 710 / 820A, SI SD 855, SDM630 SM7150 Snapdra CVE ID:	Snapdragon Congon Congon Indugon IoT, Snapdragon Solum 215, Solum	agon Au npute, nectivity sumer IG strial IG Snapdra gon Voic on Wear DM9607 8909W, CS605, SD 210/ 425, SD SD 439 , 600, SD SD 625, 675, SD , SD 820 0 845 / S 1 SDM43 10, SDX2 h_Med_2	to, /, OT, OT, agon se & rables , SD 427, / SD SD 712 / , SD SD 850, 9, 0,	securi lletins E-201 2245	#_CV		
Double Free	24-05-2019	4.6	Possibili while ru instance because missing variable Snapdra Snapdra Snapdra Mobile, Sin MDM96 MDM96 MDM96 MSM899 Qualcom	nning mes of smp of prope while use in Snape gon Come gon Indu gon IoT, Snapdrage 150, MI 107, MDM 150, MSM 166AU, QO	ultiple 2p test er protect ing glob dragon A npute, sumer IC sstrial IC Snapdra gon Voic on Wear DM9206 19640, 8909W,	ction is al Auto, OT, OT, agon ee & rables	https:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	n/20 /01/ 2019-	0-QUA- 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
Improper Restrictio n of Operatio ns within the Bounds of a Memory Buffer	24-05	-2019	4.6	212/SD SD 429, 415, SD 650/ SD 670, 845 / SD SD 845 / SD SD 845 /	SD 450, 625, SD 7 SD 820A 820A 820A 820A 820A 820A 820A 820A	SD 615/632, SD 12 / SD 835, SD 835, SD 60, SDM6  19-224 can occuries to isting by ocation or, Snaped ragon apdrago inapdrago i	16/SD 636, 710 / 5, SD DA660, 660, 7 ur if uffer in dragon n gon IoT, sic, n	https:; w.codera.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	eauro /secu in/20 ·/01/ 2019- a- ty-	0-QUA- 060619	
				CVE ID : CVE-2019-2248							
sm7150_fi	rmwar	e		Possible integer underflow can				har	1.1-		
Integer Underflo w (Wrap or Wraparo	24-05	-2019	10	happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto,				th w.qualco m m.com/c		O-QUA- 060619	
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	& CVE II	D	Pat	tch	NCIIP	C ID		
und)				Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, S in MDM96 MSM899 Qualcom 212/SD SD 430, 429, SD 615/16, 632, SD SD 710, 820A, SI SD 855, SDM630 SM7150 Snapdra	gon Con gon Con gon Indu gon IoT, Snapdrag 9206, MI 50, MSM 96AU, QO am 215, SD 205, SD SD 435, SD 450, SD 670, SD 670, SD 835, SI SDA660, SDM666, gon_Hig	nectivity sumer I ustrial IG Snapdr gon Void on Wear DM9607 8909W, CS605, SD 210/ 425, SD SD 439, 600, SD SD 625, 50 845 / S , SDM43 60, SDX2 h_Med_2	OT, OT, agon ce & rables 7, / SD 427, / SD 712 / 0, SD SD 850, 9, 0,	lletins E-201 2245	_				
Improper Input Validatio n	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				https://w.qualm.com/pany/ct-securilletins	lcom n/com produ ty/bu #_CV	0-QUA- 060619			
sxr1130_fi	rmyya	10		CVE ID : CVE-2019-2250									
	i iii wal			Kernel can write to arbitrary			Kernel can write to arbitrary			https:	//ww		
Improper Input Validatio	24-05	-2019	7.2	memory address passed by user while freeing/stopping a thread in Snapdragon Compute,			w.qua m.com pany/	lcom 1/com	0-QUA- 060619				
CV Scoring (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	cvss	D	escriptior	& CVE II	)	Pat	ch	NCIIP	C ID
n ed Sey fire	mwara		Snapdra Snapdra Snapdra SD 675, 670, SD SD 855, SXR1130	gon Indugon Mob SD 712 / 835, SD SD 8CX,	ustrial IG pile in Qu / SD 710 845 / SI SM7150	OT, CS605, / SD O 850,	ct- securi lletins E-201 2250	#_CV		
sd_8cx_firi	nware		1							
Improper Input Validatio n	24-05-2019	7.2	Kernel comemory user who thread in Snapdra Snapdra Snapdra SD 675, 670, SD SD 855, SXR1130	address ile freeir n Snapdi gon Con gon Indi gon Mob SD 712 / 835, SD SD 8CX,	s passed ng/stopp ragon Co sumer I ustrial IO pile in Qo SD 710 845 / SI SM7150	by ping a pmpute, OT, OT, CS605, O / SD O 850, O,	https:/ w.qua m.com pany/ ct- securi lletins E-201 2250	lcom n/com produ ty/bu #_CV	0-QUA- 060619	
1.04.6			CVE ID :	CVE-20	19-225	0				
sdx24_firn	nware									
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:/ w.code ra.org rity- bulleti 19/04 april-2 code- aurora securi bulleti	eauro /secu in/20 /01/ 2019-	0-QUA- 060619	
						SD				

(CVSS)

Weakness	Publis	h Date	CVSS	D	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				212/SD SD 429, 415, SD SD 650/ SD 670, 845 / SD SDM439 SDX20, S	SD 450, 625, SD 52, SD 7 SD 820A 0 850, SD 0, SDM63	SD 615/ 632, SD 12 / SD 3, SD 835 9 855, SI	16/SD 636, 710 / 5, SD DA660,				
				CVE ID :	CVE-20	19-224	7				
Redhat											
enterprise	_linux_	deskto	p								
Use After Free	22-05	-2019	9.3	Adobe F 32.0.0.1 32.0.0.1 32.0.0.1 use after Successf lead to a executio	71 and e 71 and e 71 and e free vul ful explo rbitrary n.	arlier, arlier, a arlier ha Inerabili itation c code	nd ave a ty. ould	N/A		0-RED- 060619	
enterprise	_linux_	server									
Use After Free	22-05	-2019	9.3	32.0.0.1 32.0.0.1 32.0.0.1 use after Successfi lead to a	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.		N/A		O-RED- 060619		
enterprise	_linux_	workst	ation								
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- 060619		
CV Scoring (CVSS)		0-1	1-2	2-3					7-8	8-9	9-10

Weakness	Publish	n Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
				executio	n.						
				CVE ID:	<b>CVE-20</b>	19-783	7				
Samsung											
scx-824_fi	rmware	,									
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	24-05-		4.3	Samsung allow a r Scripting that can the "prir demonst sws/sws ccessMs; CVE ID:	reflected g (XSS) v be trigg nt from f trated by sAlert.sw g msg pa	Cross-Syulnerab ered by file" feato the vs?popu aramete	iite- ility using ure, as pid=su r.	N/A		0-SAM- 060619	
Schneider	-electri	С									
modicon_p	remiur	n_firm	ware								
Informati on Exposure	22-05-	2019	5	Exposur all version M580, M Quantum Premium disclosu when re controlle	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.					O-SCH-1 060619	
Improper Check for Unusual or Exception al Condition s	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		0-SCH-1 060619		
CV Scoring (CVSS)		0-1	1-2	<b>2-3</b> 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish	Date	CVSS	D	escription	ո & CVE II	)	Pat	tch	NCIIP	C ID	
Improper Access Control	22-05-2	2019	7.5	A CWE-2 Control all version M580, M Quantur Premiur remote of overwrit settings Modbus CVE ID:	vulneral ons of the fodicon in m, and M m which code execting conf of the co	pility exi te Modic M340, Modicon could ca cution b figuration	sts in on lodicon use a by on over	N/A		O-SCH-MODI- 060619/1678		
Improper Check for Unusual or Exception al Condition s	22-05-2	2019	5	A CWE-7 for Unus Condition which con Denial of Modbus controlle Modicor versions Modicor versions firmwar Quantur Premiur	N/A		0-SCH-1 060619					
Use of Insufficie ntly Random Values	22-05-2	2019	5	CVE ID: CVE-2019-6819  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		0-SCH-1 060619		
modicon_c												
Informati	22-05-2	2019	5	A CWE-200: Information			N/A		O-SCH-I	MODI-		
CV Scoring (CVSS)		0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	1	NCIIPC ID
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 Exception al Condition s	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
CV Scoring (CVSS)		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIF	PC ID
			CVE ID :	CVE-20	19-681	.5				
Improper Control of Generatio n of Code ('Code Injection'	22-05-2019	6.4	In Modic firmwar Code Inj could ca firmwar possible using Mo	e versio ection v use an u e modifi Denial o	ns, a CW ulnerab inauthor ication v of Servic rotocol.	VE-94: ility rized vith ce when	N/A		0-SCH- 060619	
Improper Check for Unusual or Exception al Condition s	22-05-2019	5	A CWE-7 for Unus Condition which con Denial or Modbus controlle Modicon versions Modicon versions firmwar Quantum Premium CVE ID:	sual or E ons vulno ould cau f Service frames er in the a M340 - s prior to a M580 - s prior to e versio n and M n.	erability se a pos when s are sent produc firmwa V3.01, firmwa V2.80, ns of Mo odicon	nal v exists sible specific to the ts: re All odicon	N/A		O-SCH- 060619	
Use of Insufficie ntly Random Values	22-05-2019	5	CWE-33 Random which co of the TO using Et in Modic versions firmwar M340, M Modicon CVE ID:	bility, ijacking then ication tare and all odicon n,	N/A		O-SCH- 060619			
bmx-nor-0	0200h_firmwa	re								
Use of Hard- coded	22-05-2019	4	A CWE-798 use of hardcoded credentials vulnerability exists in BMX-NOR-0200H with			N/A		0-SCH-1 060619		
CV Scoring (CVSS)	()-	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	:h	NCIIPC ID
Credentia ls atv_imc_dr	r <mark>ive_controlle</mark> r	_firmv	firmware versions prior to V1.7 IR 19 which could cause a confidentiality issue when using FTP protocol.  CVE ID: CVE-2019-6812  vare			
Missing Authentic ation 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_l	mc058_firmwa	are				
Missing Authentic ation 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
CV Scoring (CVSS)		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pa	tch	NCIIP	C ID
			LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2 CVE ID : CVE-2019-6820				
modicon_l	mc078_firmwa	are					
Missing Authentic ation 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		0-SCH-I 060619	
modicon_n	n100_firmwar	е					
Missing Authentic ation 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		0-SCH-1 060619	_
CV Scoring (CVSS)		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	Pat	ch	NCIIP	C ID			
			PacDrive PacDrive		cDrive F	Pro,				
			CVE ID:	CVE-20	19-682	0				
modicon_n	n200_firmwar	e								
Missing Authentic ation for Critical Function	22-05-2019	6.4	A CWE-3 Authentic Function which co modifica configur network address) Ethernet versions Modicon ATV IMO Modicon LMC058 PacDrive PacDrive	ication for vulneral puld cause ation of detection (IF) a mask are when a terrame is of: Modical M258, Mandical Pro2	or Critical bility examinates and gatew specific son M1 Modicon Modicon Modicon Modicon Modicon Modicon CDrive F	ed in all 00, M221, c, M251, 78, Pro,	N/A		0-SCH-1 060619	
modicon_n	n241_firmwar	e								
Missing Authentic ation for Critical Function	22-05-2019	6.4	Authentic Function which comodificate configur network address) Ethernet versions Modicon ATV IMC Modicon LMC058	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,					0-SCH-I 060619	
CV Scoring (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escription	& CVE ID	Pat	ch	NCIIP	CID	
			PacDrive	e Pro2						
			CVE ID:	CVE-20	19-682	0				
modicon_n	n251_firmwar	·e								
Missing Authentic ation for Critical Function	22-05-2019	6.4	A CWE-3 Authent Function which co modifica configur network address Etherne versions Modicon ATV IMO Modicon LMC058 PacDrive PacDrive	ication for vulneral puld cause attion of cation (IF) a mask and the frame in M200, IF and M258,	or Critica ability ex se a levice IP address ad gatew specific s receive icon M1 Modicon Modicon Modicon on LMCO cDrive P	cists  S,  Vay IP  ed in all  00,  M221,  T,  M251,  78,  ro,	N/A		O-SCH-I 060619	
modicon_n	n258_firmwar	·e								
Missing Authentic ation for Critical Function	22-05-2019	6.4	A CWE-3 Authent Function which co modifica configur network address) Etherne versions Modicor ATV IMO Modicor LMC058 PacDrive	ication for vulneral puld cause attion of cation (IF) amask and the frame in the frame in M200, IF amage and M258, IF amage and	or Critical ability examples and levice IP address and gatew specific son M1 and	ed in all 00, M221, 5, M251, 78,	N/A		O-SCH-I 060619	

Weakness	Publish Date	cvss	D	escription	& CVE II	)	Pat	ch	NCIIP	C ID
			CVE ID :	CVE-20	19-682	0				
pacdrive_e	co_firmware	1								
Missing Authentic ation for Critical Function	hentic n for ical  6.4  Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221,						N/A		0-SCH-I 060619	
pacdrive_p	ro2_firmware	•								
Missing Authentic ation for Critical Function	22-05-2019	6.4	A CWE-3 Authent Function which co modificat configur network address) Etherne versions Modicor ATV IMO Modicor LMC058 PacDrive PacDrive	ication for vulneral puld cause attion of cation (IF) amask and the frame is of: Moda M200, IF amask and M258, IF amask and M25	or Critic ability ex se a levice IP addres ad gatew specific s receive icon M1 Modicon Modicon Modicon CDrive F	ed in all 00, M221, M251, M251, Pro,	N/A		0-SCH-I 060619	
			l				<u> </u>			

Weakness	Publis	h Date	cvss	De	escription	& CVE II	)	Pat	tch	NCIIP	C ID
pacdrive_p	oro_firn	nware						•			
Missing Authentic ation for Critical Function	22-05-	-2019	6.4	A CWE-3 Authent Function which co modifica configur network address) Etherner versions Modicon ATV IMO Modicon LMC058 PacDrive PacDrive	ication for vulneral ould cause attion of cation (IF) a mask and the frame in M200, IF and M258,	or Criticability exists a levice IFP address address received icon M1 Modicon Modicon Modicon LMCO cDrive F	N/A		0-SCH-I 060619		
modicon_n	n340_fi	irmwar	e								
Use of Insufficie ntly Random Values	22-05-	-2019	5	CWE-33 Random which co of the TO using Et in Modio versions firmwar M340, M Modicon CVE ID:	Values vould cause thernet con M58 prior to e version Iodicon I	vulnerable the his ection who ommunion of the version of Moremium m.	pility, jacking hen cation are and all dicon	N/A		O-SCH-I 060619	
modicon_n	n221_fi	irmwar	e								
Missing Authentic ation 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-I 060619	
CV Scoring (CVSS)		0-1	1-2	<b>2-3</b> 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	De	escription	n & CVE II	Pat	tch	NCIIP	C ID	
Tp-link				address) Etherner versions Modicon ATV IMC Modicon LMC058 PacDrive PacDrive	t frame i s of: Mod a M200, I drive co a M241, I a M258, I de Eco ,Pa e Pro2	s receive licon M1 Modicor ontrolle Modicor Modicor on LMC0					
tl-wr840n	firmw	are									
Improper Neutraliz ation of Input During Web Page Generatio n ('Cross- site Scripting' )	24-05	-2019	3.5	TP-Link 0000000 via the n attacker router b passwor admin lo HYDRA t name. W network automat connecti All the u disconne	of device the sected from the	es allow name. T g into the ng the oing to the e by THO e netwo SS paylo hanged ad the in disconne om the in	he he C- rk bad, the ternet ected.	N/A		0-TPT 060619	
vstracam											
c38s_firmv	ware										
Improper Authentic ation	23-05	-2019	10	An issue upgrade VStarcar CH-sys-4200V (C) 48.53.20 remote c executed firmwar	re.cgi or (C7824V .119~12 -sys- 123 dev d can be h a syste	VIP) 23 and ices. A	N/A		0-VST-0 060619		
CV Scoring (CVSS)		0-1	1-2	2-3	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	D	escription	n & CVE II	Pa	tch	NCIIP	CID	
			can mod internal account executir	ication. The faction of the fact the fa	iles with re or eve tion by mand.					
c7824wip	_firmware									
Improper Authentic ation	23-05-2019	10	VStarcar CH-sys-4 200V (C 48.53.20 remote executed firmwar authent can mod internal account executir	e_firmwa m 100T 48.53.75 (38S) CH 03.119~ comman d throug	re.cgi or (C7824V).119~123 develor attacking without the or even tion by mand.	NIP) 23 and ices. A e em at cker ain the en steal	N/A		0-VST-0 060619	
vstracm	waro									
Improper Authentic ation	23-05-2019	7.5	upgrade 100T (C KR75.8. KR203.1 web ser account manipul firmwar authent can achi through firmwar	e was dise htmls.co. 7824WI 53.20 and less can lated three access a manipe e update access a manipe e update coupdate coupage	gi on VSP) d 200V levices. The ough a vertice without the oulated vertices.	Ctarcam (C38S) The nd web UI at any cker e device web UI	N/A		0-VST-0 060619	
CV Scoring	Scale									
CV Scoring		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c7824iwp_firmware					
Improper Authentic ation	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 Wraparo und	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://ww w.windriver .com/feeds/ wind_river_ security_not ices.xml	O-WIN- VXWO- 060619/1707