National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 31 Mar 2020 Vol. 07 No. 06

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
acyba					
acymailing					
Unrestricted Upload of File with Dangerous Type	24-03-2020	6.5	Acyba AcyMailing before 6.9.2 mishandles file uploads by admins. **CVE ID : CVE-2020-10934**	N/A	A-ACY-ACYM-070420/1
Adobe					
experience_manager					
Server-Side Request Forgery (SSRF)	25-03-2020	5	Adobe Experience Manager versions 6.5 and earlier have a server-side request forgery (ssrf) vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2020-3769**	https://helpx.adobe.com/security/products/experience-manager/apsb20-15.html	A-ADO-EXPE-070420/2
acrobat_dc					
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/3

CVSS 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
			code execution . **CVE ID : CVE-2020-3792**		
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3793**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/4
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3795**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/5
Improper Restriction of Operations within the Bounds of a Memory	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			earlier, and 2015.006.30510 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3797**		
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3799**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/7
Improper Release of Memory Before Removing Last Reference	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory address leak vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3800**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/8
Use After	25-03-2020	7.5	Adobe Acrobat and Reader	https://help	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3801**	x.adobe.com /security/products/acrobat/apsb20-13.html	070420/9
Use After Free	25-03-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3802**	https://helpx.adobe.com /security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/10
Untrusted Search Path	25-03-2020	4.4	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an insecure library loading (dll	https://helpx.adobe.com /security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/11

CVSS 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
			hijacking) vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-3803**		
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3804**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/12
Use After Free	25-03-2020	10	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3805**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/13
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and	https://helpx.adobe.com/security/products/acro	A-ADO-ACRO-070420/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3806**	bat/apsb20-13.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3807**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/15
acrobat_reader_dc					
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution . **CVE ID : CVE-2020-3792**		
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3793**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/17
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3795**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/18
Improper Restriction of Operations within the Bounds of a Memory	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			earlier, and 2015.006.30510 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3797**		
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3799**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/20
Improper Release of Memory Before Removing Last Reference	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory address leak vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3800**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/21
Use After	25-03-2020	7.5	Adobe Acrobat and Reader	https://help	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3801**	x.adobe.com /security/products/acrobat/apsb20-13.html	070420/22
Use After Free	25-03-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3802**	https://helpx.adobe.com /security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/23
Untrusted Search Path	25-03-2020	4.4	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an insecure library loading (dll	https://helpx.adobe.com /security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/24

CVSS 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
			hijacking) vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-3803**		
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3804**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/25
Use After Free	25-03-2020	10	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3805**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/26
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and	https://helpx.adobe.com/security/products/acro	A-ADO-ACRO-070420/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3806**	bat/apsb20-13.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3807**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	A-ADO-ACRO-070420/28
coldfusion					
Information Exposure	25-03-2020	5	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have a remote file read vulnerability. Successful exploitation could lead to arbitrary file read from the coldfusion install directory. **CVE ID : CVE-2020-3761**	https://helpx.adobe.com/security/products/coldfusion/apsb20-16.html	A-ADO-COLD-070420/29
Improper Input	25-03-2020	10	ColdFusion versions ColdFusion 2016, and	https://helpx.adobe.com	A-ADO-COLD-070420/30

CVSS 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
Validation			ColdFusion 2018 have a file inclusion vulnerability. Successful exploitation could lead to arbitrary code execution of files located in the webroot or its subdirectory. **CVE ID : CVE-2020-3794**	/security/products/coldfusion/apsb20-16.html	
creative_cloud					
Time-of-check Time-of-use (TOCTOU) Race Condition	25-03-2020	5.8	Creative Cloud Desktop Application versions 5.0 and earlier have a time-of-check to time-of-use (toctou) race condition vulnerability. Successful exploitation could lead to arbitrary file deletion. **CVE ID : CVE-2020-3808**	https://helpx.adobe.com/security/products/creative-cloud/apsb20-11.html	A-ADO-CREA-070420/31
photoshop_cc					
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3770**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/32
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3771		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3772**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/34
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3773**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/35
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3774**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/36
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/37

CVSS 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
			code execution. **CVE ID : CVE-2020-3775**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3776**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/38
Out-of-bounds Read	25-03-2020	5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3777**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/39
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3778**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/40
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-3779**		
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3780**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/42
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3781**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/43
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3782**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/44
Improper Restriction of Operations within the Bounds of a Memory	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a heap corruption vulnerability. Successful exploitation	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			could lead to arbitrary code execution. **CVE ID : CVE-2020-3783**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3784**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/46
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3785**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/47
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3786**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/48
Improper Restriction of Operations within the Bounds of a	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability.	https://helpx.adobe.com/security/products/photoshop/apsb	A-ADO-PHOT-070420/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3787**	20-14.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3788**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/50
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3789**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/51
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3790**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/52
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-	https://helpx.adobe.com/security/products/photoshop/apsb	A-ADO-PHOT-070420/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3791**	20-14.html	
bridge					
Out-of-bounds Write	25-03-2020	6.8	Adobe Bridge versions 10.0 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9551**	https://helpx.adobe.com/security/products/bridge/apsb20-17.html	A-ADO-BRID-070420/54
Out-of-bounds Write	25-03-2020	6.8	Adobe Bridge versions 10.0 have a heap-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9552**	https://helpx.adobe.com/security/products/bridge/apsb20-17.html	A-ADO-BRID-070420/55
genuine_integrity_service					
Incorrect Default Permissions	25-03-2020	7.5	Adobe Genuine Integrity Service versions Version 6.4 and earlier have an insecure file permissions vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-3766**	https://helpx.adobe.com/security/products/integrity_service/apsb20-12.html	A-ADO-GENU-070420/56
photoshop_2020					
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution. **CVE ID : CVE-2020-3770**		
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3771**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/58
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3772**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/59
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3773**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/60
Improper Restriction of Operations within the Bounds of a Memory	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			could lead to arbitrary code execution. **CVE ID : CVE-2020-3774**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3775**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/62
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3776**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/63
Out-of-bounds Read	25-03-2020	5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3777**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/64
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/photoshop/apsb	A-ADO-PHOT-070420/65

CVSS 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
			information disclosure. **CVE ID : CVE-2020-3778**	20-14.html	
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3779**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/66
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3780**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/67
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3781**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/68
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to information disclosure. **CVE ID : CVE-2020-3782**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a heap corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3783**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/70
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3784**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/71
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3785**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/72
Improper Restriction of Operations within the Bounds of a	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability.	https://helpx.adobe.com/security/products/photoshop/apsb	A-ADO-PHOT-070420/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3786**	20-14.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3787**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/74
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3788**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/75
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3789**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/76
Improper Restriction of Operations within the	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory	https://helpx.adobe.com/security/products/photoshop/apsb	A-ADO-PHOT-070420/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3790**	20-14.html	
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3791**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	A-ADO-PHOT-070420/78
Apache					
traffic_server					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	23-03-2020	7.5	There is a vulnerability in Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.8, and 8.0.0 to 8.0.5 with a smuggling attack and Transfer-Encoding and Content length headers. Upgrade to versions 7.1.9 and 8.0.6 or later versions. **CVE ID : CVE-2020-1944**	N/A	A-APA-TRAF-070420/79
tika					
Uncontrolled Resource Consumption	23-03-2020	4.3	A carefully crafted or corrupt PSD file can cause excessive memory usage in Apache Tika's PSDParser in versions 1.0-1.23. **CVE ID : CVE-2020-1950**	https://lists.apache.org/thread.html/r463b1a67817ae55fe022536edd6db34e8f9636971188430cbcf8a8dd%40%3Cdev.tika.	A-APA-TIKA-070420/80

CVSS 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
				apache.org%3E	
Loop with Unreachable Exit Condition ('Infinite Loop')	23-03-2020	4.3	A carefully crafted or corrupt PSD file can cause an infinite loop in Apache Tika's PSDParser in versions 1.0-1.23. **CVE ID : CVE-2020-1951**	N/A	A-APA-TIKA-070420/81
aquaforest					
tiff_server					
Information Exposure	18-03-2020	5	Aquaforest TIFF Server 4.0 allows Unauthenticated File and Directory Enumeration via tiffserver/tssp.aspx. **CVE ID : CVE-2020-9323**	N/A	A-AQU-TIFF-070420/82
Insufficiently Protected Credentials	18-03-2020	5	Aquaforest TIFF Server 4.0 allows Unauthenticated SMB Hash Capture via UNC. **CVE ID : CVE-2020-9324**	N/A	A-AQU-TIFF-070420/83
Improper Input Validation	18-03-2020	5	Aquaforest TIFF Server 4.0 allows Unauthenticated Arbitrary File Download. **CVE ID : CVE-2020-9325**	N/A	A-AQU-TIFF-070420/84
ARM					
mbed_crypto					
Missing Encryption of Sensitive Data	24-03-2020	4.3	Arm Mbed TLS before 2.6.15 allows attackers to obtain sensitive information (an RSA private key) by measuring cache usage during an import. **CVE ID : CVE-2020-10941**	N/A	A-ARM-MBED-070420/85

CVSS 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
mbed_tls					
Missing Encryption of Sensitive Data	24-03-2020	4.3	Arm Mbed TLS before 2.6.15 allows attackers to obtain sensitive information (an RSA private key) by measuring cache usage during an import. **CVE ID : CVE-2020-10941**	N/A	A-ARM-MBED-070420/86
armorx					
lisomail					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-03-2020	7.5	LisoMail, by ArmorX, allows SQL Injections, attackers can access the database without authentication via a URL parameter manipulation. **CVE ID : CVE-2020-3922**	N/A	A-ARM-LISO-070420/87
Artica					
pandora_fms					
Unrestricted Upload of File with Dangerous Type	16-03-2020	6.5	index.php?sec=godmode/extensions&sec2=extensions/files_repo in Pandora FMS v7.0 NG allows authenticated administrators to upload malicious PHP scripts, and execute them via base64 decoding of the file location. This affects v7.0NG.742_FIX_PERL2020. **CVE ID : CVE-2020-5844**	N/A	A-ART-PAND-070420/88
Unrestricted Upload of	23-03-2020	6.5	Artica Pandora FMS through 7.42 is vulnerable	N/A	A-ART-PAND-070420/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			to remote PHP code execution because of an Unrestricted Upload Of A File With A Dangerous Type issue in the File Manager. An attacker can create a (or use an existing) directory that is externally accessible to store PHP files. The filename and the exact path is known by the attacker, so it is possible to execute PHP code in the context of the application. The vulnerability is exploitable only with Administrator access. **CVE ID : CVE-2020-7935**		
Information Exposure	23-03-2020	5	In Artica Pandora FMS through 7.42, an unauthenticated attacker can read the chat history. The file is in JSON format and it contains user names, user IDs, private messages, and timestamps. **CVE ID : CVE-2020-8497**	N/A	A-ART-PAND-070420/90
Unrestricted Upload of File with Dangerous Type	23-03-2020	6.5	In Artica Pandora FMS through 7.42, Web Admin users can execute arbitrary code by uploading a .php file via the File Repository component, a different issue than CVE-2020-7935 and CVE-2020-8500. **CVE ID : CVE-2020-8511**	N/A	A-ART-PAND-070420/91

CVSS 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
articatech					
artica_proxy					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-03-2020	6.5	Artica Proxy 4.26 allows remote command execution for an authenticated user via shell metacharacters in the "Modify the hostname" field. **CVE ID : CVE-2020-10818**	N/A	A-ART-ARTI-070420/92
Atlassian					
subversion_application_lifecycle_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-03-2020	4.3	Subversion ALM for the enterprise before 8.8.2 allows reflected XSS at multiple locations. **CVE ID : CVE-2020-9344**	N/A	A-ATL-SUBV-070420/93
Atutor					
acontent					
Unrestricted Upload of File with Dangerous Type	16-03-2020	6.5	An issue was discovered in AContent through 1.4. It allows the user to run commands on the server with a low-privileged account. The upload section in the file manager page contains an arbitrary file upload vulnerability via upload.php. The extension .php7 bypasses file upload restrictions. **CVE ID : CVE-2020-10557**	N/A	A-ATU-ACON-070420/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
beyondtrust					
privilege_management_for_windows_and_mac					
Improper Input Validation	18-03-2020	5	BeyondTrust Privilege Management for Windows and Mac (aka PMWM; formerly Avecto Defendpoint) 5.1 through 5.5 before 5.5 SR1 mishandles command-line arguments with PowerShell .ps1 file extensions present, leading to a DefendpointService.exe crash. **CVE ID : CVE-2020-9326**	https://www.beyondtrust.com/support/changelog/privilege-management-for-windows-5-5-sr1	A-BEY-PRIV-070420/95
blamer_project					
blamer					
Improper Control of Generation of Code ('Code Injection')	20-03-2020	7.5	Code injection vulnerability in blamer 1.0.0 and earlier may result in remote code execution when the input can be controlled by an attacker. **CVE ID : CVE-2020-8137**	N/A	A-BLA-BLAM-070420/96
centos-webpanel					
centos_web_panel					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-03-2020	7.5	CentOS-WebPanel.com (aka CWP) CentOS Web Panel (for CentOS 6 and 7) allows SQL Injection via the /cwp_{SESSION_HASH}/admin/loader_ajax.php term parameter. **CVE ID : CVE-2020-**	N/A	A-CEN-CENT-070420/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10230		
cesnet					
perun					
Incorrect Permission Assignment for Critical Resource	25-03-2020	5	In Perun before version 3.9.1, VO or group manager can modify configuration of the LDAP extSource to retrieve all from Perun LDAP. Issue is fixed in version 3.9.1 by sanitisation of the input. **CVE ID : CVE-2020-5281**	https://github.com/CESNET/perun/security/advisories/GHSA-gj88-9q3f-72m3	A-CES-PERU-070420/98
Citrix					
citrix_sd-wan_center					
Improper Certificate Validation	16-03-2020	4.3	Citrix SD-WAN 10.2.x before 10.2.6 and 11.0.x before 11.0.3 has Missing SSL Certificate Validation. **CVE ID : CVE-2020-6175**	https://support.citrix.com/article/CTX263526	A-CIT-CITR-070420/99
netscaler_sd-wan_center					
Improper Certificate Validation	16-03-2020	4.3	Citrix SD-WAN 10.2.x before 10.2.6 and 11.0.x before 11.0.3 has Missing SSL Certificate Validation. **CVE ID : CVE-2020-6175**	https://support.citrix.com/article/CTX263526	A-CIT-NETS-070420/100
Cmsmadesimple					
cms_made_simple					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-03-2020	3.5	The Filemanager in CMS Made Simple 2.2.13 has stored XSS via a .pxd file, as demonstrated by m1_files[] to admin/moduleinterface.php. **CVE ID : CVE-2020-10681**	N/A	A-CMS-CMS_-070420/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	20-03-2020	6.8	The Filemanager in CMS Made Simple 2.2.13 allows remote code execution via a .php.jpegd JPEG file, as demonstrated by m1_files[] to admin/moduleinterface.php. The file should be sent as application/octet-stream and contain PHP code (it need not be a valid JPEG file). **CVE ID : CVE-2020-10682**	N/A	A-CMS-CMS_-070420/102
Codeigniter					
codeigniter					
Improper Privilege Management	23-03-2020	6.5	** DISPUTED ** CodeIgniter through 4.0.0 allows remote attackers to gain privileges via a modified Email ID to the "Select Role of the User" page. NOTE: A contributor to the CodeIgniter framework argues that the issue should not be attributed to CodeIgniter. Furthermore, the blog post reference shows an unknown website built with the CodeIgniter framework but that CodeIgniter is not responsible for introducing this issue because the framework has never provided a login screen, nor any kind of login or user management facilities beyond a Session	N/A	A-COD-CODE-070420/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			library. **CVE ID : CVE-2020-10793**		
containous					
traefik					
Improper Certificate Validation	16-03-2020	5	configurationwatcher.go in Traefik 2.x before 2.1.4 and TraefikEE 2.0.0 mishandles the purging of certificate contents from providers before logging. **CVE ID : CVE-2020-9321**	N/A	A-CON-TRAE-070420/104
Cpanel					
cpanel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-03-2020	4.3	cPanel before 84.0.20 allows self XSS via a temporary character-set specification (SEC-515). **CVE ID : CVE-2020-10113**	N/A	A-CPA-CPAN-070420/105
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-03-2020	4.3	cPanel before 84.0.20 allows stored self-XSS via the HTML file editor (SEC-535). **CVE ID : CVE-2020-10114**	N/A	A-CPA-CPAN-070420/106
Improper Input Validation	17-03-2020	9	cPanel before 84.0.20, when PowerDNS is used, allows arbitrary code execution as root via dnsadmin. (SEC-537). **CVE ID : CVE-2020-10115**	N/A	A-CPA-CPAN-070420/107

CVSS 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
Incorrect Authorization	17-03-2020	5	cPanel before 84.0.20 allows attackers to bypass intended restrictions on features and demo accounts via WebDisk UAPI calls (SEC-541). **CVE ID : CVE-2020-10116**	N/A	A-CPA-CPAN-070420/108
Incorrect Authorization	17-03-2020	6.4	cPanel before 84.0.20 mishandles enforcement of demo checks in the Market UAPI namespace (SEC-542). **CVE ID : CVE-2020-10117**	N/A	A-CPA-CPAN-070420/109
N/A	17-03-2020	6.4	cPanel before 84.0.20 allows a demo account to modify files via Branding API calls (SEC-543). **CVE ID : CVE-2020-10118**	N/A	A-CPA-CPAN-070420/110
N/A	17-03-2020	7.5	cPanel before 84.0.20 allows a demo account to achieve remote code execution via a cpsrvd rsync shell (SEC-544). **CVE ID : CVE-2020-10119**	N/A	A-CPA-CPAN-070420/111
Incorrect Authorization	17-03-2020	9	cPanel before 84.0.20 allows resellers to achieve remote code execution as root via a cpsrvd rsync shell (SEC-545). **CVE ID : CVE-2020-10120**	N/A	A-CPA-CPAN-070420/112
N/A	17-03-2020	7.5	cPanel before 84.0.20 allows a demo account to achieve code execution via	N/A	A-CPA-CPAN-070420/113

CVSS 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
			PassengerApps APIs (SEC-546). **CVE ID : CVE-2020-10121**		
Improper Input Validation	17-03-2020	6.4	cPanel before 84.0.20 allows a webmail or demo account to delete arbitrary files (SEC-547). **CVE ID : CVE-2020-10122**	N/A	A-CPA-CPAN-070420/114
Cutephp					
cutenews					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	4.3	Cross-site scripting vulnerability in CuteNews 2.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2020-5557**	N/A	A-CUT-CUTE-070420/115
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-03-2020	9	CuteNews 2.0.1 allows remote authenticated attackers to execute arbitrary PHP code via unspecified vectors. **CVE ID : CVE-2020-5558**	N/A	A-CUT-CUTE-070420/116
deltaww					
cncsoft_screeneditor					
Out-of-bounds Read	18-03-2020	4.3	Delta Industrial Automation CNCSoft ScreenEditor, v1.00.96 and prior. An out-of-bounds read overflow can be exploited when a valid user opens a specially	N/A	A-DEL-CNCS-070420/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted, malicious input file due to the lack of validation. **CVE ID : CVE-2020-6976**		
Out-of-bounds Write	18-03-2020	6.8	Delta Industrial Automation CNCSoft ScreenEditor, v1.00.96 and prior. Multiple stack-based buffer overflows can be exploited when a valid user opens a specially crafted, malicious input file. **CVE ID : CVE-2020-7002**	N/A	A-DEL-CNCS-070420/118
denx					
u-boot					
Improper Input Validation	19-03-2020	6.8	Das U-Boot through 2020.01 allows attackers to bypass verified boot restrictions and subsequently boot arbitrary images by providing a crafted FIT image to a system configured to boot the default configuration. **CVE ID : CVE-2020-10648**	N/A	A-DEN-U-BO-070420/119
Docker					
desktop					
Improper Privilege Management	18-03-2020	7.2	Docker Desktop allows local privilege escalation to NT AUTHORITY\SYSTEM because it mishandles the collection of diagnostics with Administrator privileges, leading to	N/A	A-DOC-DESK-070420/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary DACL permissions overwrites and arbitrary file writes. This affects Docker Desktop Enterprise before 2.1.0.9, Docker Desktop for Windows Stable before 2.2.0.4, and Docker Desktop for Windows Edge before 2.2.2.0. **CVE ID : CVE-2020-10665**		
dogtagpki					
dogtagpki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-03-2020	3.5	A flaw was found in the all pki-core 10.x.x versions, where Token Processing Service (TPS) where it did not properly sanitize Profile IDs, enabling a Stored Cross-Site Scripting (XSS) vulnerability when the profile ID is printed. An attacker with sufficient permissions could trick an authenticated victim into executing a specially crafted Javascript code. **CVE ID : CVE-2020-1696**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1696	A-DOG-DOGT-070420/121
easybuild_project					
easybuild					
Insecure Storage of Sensitive Information	19-03-2020	2.1	In EasyBuild before version 4.1.2, the GitHub Personal Access Token (PAT) used by EasyBuild for the GitHub integration features (like `--new-pr`, `--fro,-pr`, etc.) is shown in plain text in EasyBuild	https://github.com/easybuilders/easybuild-framework/security/advisories/GHSA-2wx6-	A-EAS-EASY-070420/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			debug log files. This issue is fixed in EasyBuild v4.1.2, and in the `master`+ `develop` branches of the `easybuild-framework` repository. **CVE ID : CVE-2020-5262**	wc87-rmjm	
Eaton					
ups_companion					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	5.8	UPS companion software v1.05 & Prior is affected by 'Eval Injection' vulnerability. The software does not neutralize or incorrectly neutralizes code syntax before using the input in a dynamic evaluation call e.g."eval" in "Update Manager" class when software attempts to see if there are updates available. This results in arbitrary code execution on the machine where software is installed. **CVE ID : CVE-2020-6650**	N/A	A-EAT-UPS_-070420/123
EMC					
rsa_authentication_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-03-2020	3.5	RSA Authentication Manager versions prior to 8.4 P10 contain a stored cross-site scripting vulnerability in the Security Console. A malicious RSA Authentication Manager Security Console	N/A	A-EMC-RSA_-070420/124

CVSS 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
			administrator with advanced privileges could exploit this vulnerability to store arbitrary HTML or JavaScript code through the Security Console web interface. When other Security Console administrators open the affected report page, the injected scripts could potentially be executed in their browser. **CVE ID : CVE-2020-5339**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-03-2020	3.5	RSA Authentication Manager versions prior to 8.4 P10 contain a stored cross-site scripting vulnerability in the Security Console. A malicious RSA Authentication Manager Security Console administrator with advanced privileges could exploit this vulnerability to store arbitrary HTML or JavaScript code through the Security Console web interface. When other Security Console administrators attempt to change the default security domain mapping, the injected scripts could potentially be executed in their browser. **CVE ID : CVE-2020-5340**	N/A	A-EMC-RSA_-070420/125
entrustdatacard					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
entelligence_security_provider					
Improper Certificate Validation	18-03-2020	4	Entrust Entelligence Security Provider (ESP) before 10.0.60 on Windows mishandles errors during SSL Certificate Validation, leading to situations where (for example) a user continues to interact with a web site that has an invalid certificate chain. **CVE ID : CVE-2020-10659**	N/A	A-ENT-ENTE-070420/126
EZ					
ez_publish-kernel					
Unrestricted Upload of File with Dangerous Type	22-03-2020	7.5	eZ Publish Kernel before 5.4.14.1, 6.x before 6.13.6.2, and 7.x before 7.5.6.2 and eZ Publish Legacy before 5.4.14.1, 2017 before 2017.12.7.2, and 2019 before 2019.03.4.2 allow remote attackers to execute arbitrary code by uploading PHP code, unless the vhost configuration permits only app.php execution. **CVE ID : CVE-2020-10806**	N/A	A-EZ-EZ_P-070420/127
ez_publish-legacy					
Unrestricted Upload of File with Dangerous Type	22-03-2020	7.5	eZ Publish Kernel before 5.4.14.1, 6.x before 6.13.6.2, and 7.x before 7.5.6.2 and eZ Publish Legacy before 5.4.14.1, 2017 before 2017.12.7.2,	N/A	A-EZ-EZ_P-070420/128

CVSS 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
			and 2019 before 2019.03.4.2 allow remote attackers to execute arbitrary code by uploading PHP code, unless the vhost configuration permits only app.php execution. **CVE ID : CVE-2020-10806**		
F5					
big-ip_access_policy_manager					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/129
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/130
big-ip_advanced_firewall_manager					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/131
Improper Input	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may	N/A	A-F5-BIG--070420/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			cause TMM to produce a core file. **CVE ID : CVE-2020-5859**		
big-ip_analytics					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/133
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/134
big-ip_application_acceleration_manager					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/135
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/136
big-ip_application_security_manager					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and	N/A	A-F5-BIG--070420/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**		
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/138
big-ip_domain_name_system					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/139
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/140
big-ip_edge_gateway					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/141
big-ip_fraud_protection_service					
Improper	27-03-2020	5	On BIG-IP 15.0.0-15.0.1,	N/A	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**		070420/142
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/143
big-ip_global_traffic_manager					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/144
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/145
big-ip_link_controller					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/147
big-ip_local_traffic_manager					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/148
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/149
big-ip_policy_enforcement_manager					
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/150
Improper Input Validation	27-03-2020	5	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file. **CVE ID : CVE-2020-5859**	N/A	A-F5-BIG--070420/151
big-ip_webaccelerator					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	27-03-2020	5	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service. **CVE ID : CVE-2020-5857**	N/A	A-F5-BIG--070420/152
Fasterxml					
jackson-databind					
Deserialization of Untrusted Data	26-03-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.aoju.bus.proxy.provider.remoting.RmiProvider (aka bus-proxy). **CVE ID : CVE-2020-10968**	N/A	A-FAS-JACK-070420/153
N/A	18-03-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.aries.transaction.jms.internal.XaPooledConnectionFactory (aka aries.transaction.jms). **CVE ID : CVE-2020-10672**	N/A	A-FAS-JACK-070420/154
N/A	18-03-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to	N/A	A-FAS-JACK-070420/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			com.caucho.config.types.ResourceRef (aka caucho-quercus). **CVE ID : CVE-2020-10673**		
fastify					
fastify-multipart					
Uncontrolled Resource Consumption	20-03-2020	5	Prototype pollution vulnerability in fastify-multipart < 1.0.5 allows an attacker to crash fastify applications parsing multipart requests by sending a specially crafted request. **CVE ID : CVE-2020-8136**	N/A	A-FAS-FAST-070420/156
Fortinet					
fortiweb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-03-2020	3.5	An improper neutralization of input vulnerability in FortiWeb allows a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the Disclaimer Description of a Replacement Message. **CVE ID : CVE-2020-6646**	N/A	A-FOR-FORT-070420/157
Foxitsoftware					
foxit_studio_photo					
Out-of-bounds Read	20-03-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is	N/A	A-FOX-FOXI-070420/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9624. **CVE ID : CVE-2020-8877**		
Out-of-bounds Write	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the	N/A	A-FOX-FOXI-070420/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. Was ZDI-CAN-9625. **CVE ID : CVE-2020-8878**		
Out-of-bounds Read	20-03-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9626. **CVE ID : CVE-2020-8879**	N/A	A-FOX-FOXI-070420/160
Out-of-bounds Read	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a	N/A	A-FOX-FOXI-070420/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9773. **CVE ID : CVE-2020-8880**		
Use After Free	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9774. **CVE ID : CVE-2020-8881**	N/A	A-FOX-FOXI-070420/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the PSD files. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9811. **CVE ID : CVE-2020-8882**	N/A	A-FOX-FOXI-070420/163
Out-of-bounds Read	20-03-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past	N/A	A-FOX-FOXI-070420/164

CVSS 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
			the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9880. **CVE ID : CVE-2020-8883**		
frozennode					
laravel-administrator					
Unrestricted Upload of File with Dangerous Type	25-03-2020	6.5	FrozenNode Laravel-Administrator through 5.0.12 allows unrestricted file upload (and consequently Remote Code Execution) via admin/tips_image/image/file_upload image upload with PHP content within a GIF image that has the .php extension. NOTE: this product is discontinued. **CVE ID : CVE-2020-10963**	N/A	A-FRO-LARA-070420/165
ghost					
ghost					
Server-Side Request Forgery (SSRF)	20-03-2020	5.5	Server-side request forgery (SSRF) vulnerability in Ghost CMS < 3.10.0 allows an attacker to scan local or external network or otherwise interact with internal systems. **CVE ID : CVE-2020-8134**	N/A	A-GHO-GHOS-070420/166
Golang					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
go					
Improper Certificate Validation	16-03-2020	7.8	Go before 1.12.16 and 1.13.x before 1.13.7 (and the crypto/cryptobyte package before 0.0.0-20200124225646-8b5121be2f68 for Go) allows attacks on clients (resulting in a panic) via a malformed X.509 certificate. **CVE ID : CVE-2020-7919**	https://groups.google.com/forum/#!topic/golang-announce/Hsw4mHYc470, https://security.netapp.com/advisory/ntap-20200327-0001/	A-GOL-GO-070420/167
Google					
chrome					
Improper Input Validation	23-03-2020	6.8	Insufficient policy enforcement in media in Google Chrome prior to 80.0.3987.132 allowed a remote attacker to bypass same origin policy via a crafted HTML page. **CVE ID : CVE-2020-6420**	N/A	A-GOO-CHRO-070420/168
Use After Free	23-03-2020	9.3	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6422**	N/A	A-GOO-CHRO-070420/169
Use After Free	23-03-2020	9.3	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted	N/A	A-GOO-CHRO-070420/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML page. **CVE ID : CVE-2020-6424**		
Improper Input Validation	23-03-2020	5.8	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.149 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension. **CVE ID : CVE-2020-6425**	N/A	A-GOO-CHRO-070420/171
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-03-2020	4.3	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6426**	N/A	A-GOO-CHRO-070420/172
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6427**	N/A	A-GOO-CHRO-070420/173
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6428**	N/A	A-GOO-CHRO-070420/174
Use After	23-03-2020	9.3	Use after free in audio in	N/A	A-GOO-CHRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6429**		070420/175
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6449**	N/A	A-GOO-CHRO-070420/176
Graphicsmagick					
graphicsmagick					
Integer Overflow or Wraparound	24-03-2020	7.5	GraphicsMagick before 1.3.35 has an integer overflow and resultant heap-based buffer overflow in HuffmanDecodeImage in magick/compress.c. **CVE ID : CVE-2020-10938**	N/A	A-GRA-GRAP-070420/177
hashicorp					
vault					
Incorrect Default Permissions	23-03-2020	4.3	HashiCorp Vault and Vault Enterprise versions 0.9.0 through 1.3.3 may, under certain circumstances, have an Entity's Group membership inadvertently include Groups the Entity no longer has permissions to. Fixed in 1.3.4. **CVE ID : CVE-2020-**	https://github.com/hashicorp/vault/blob/master/CHANGELOG.md#134-march-19th-2020	A-HAS-VAUL-070420/178

CVSS 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
			10660		
N/A	23-03-2020	5.8	HashiCorp Vault and Vault Enterprise versions 0.11.0 through 1.3.3 may, under certain circumstances, have existing nested-path policies grant access to Namespaces created after-the-fact. Fixed in 1.3.4. **CVE ID : CVE-2020-10661**	https://github.com/hashicorp/vault/blob/master/CHANGELOG.md#134-march-19th-2020	A-HAS-VAUL-070420/179
Hdfgroup					
hdf5					
Out-of-bounds Write	22-03-2020	4.3	An issue was discovered in HDF5 through 1.12.0. A heap-based buffer overflow exists in the function Decompress() located in decompress.c. It can be triggered by sending a crafted file to the gif2h5 binary. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2020-10809**	N/A	A-HDF-HDF5-070420/180
NULL Pointer Dereference	22-03-2020	4.3	An issue was discovered in HDF5 through 1.12.0. A NULL pointer dereference exists in the function H5AC_unpin_entry() located in H5AC.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2020-10810**	N/A	A-HDF-HDF5-070420/181
Out-of-bounds Read	22-03-2020	4.3	An issue was discovered in HDF5 through 1.12.0. A	N/A	A-HDF-HDF5-070420/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			heap-based buffer over-read exists in the function H5O__layout_decode() located in H5Olayout.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2020-10811**		
NULL Pointer Dereference	22-03-2020	5	An issue was discovered in HDF5 through 1.12.0. A NULL pointer dereference exists in the function H5F_get_nrefs() located in H5Fquery.c. It allows an attacker to cause Denial of Service. **CVE ID : CVE-2020-10812**	N/A	A-HDF-HDF5-070420/183
Honeywell					
notifier_webserver					
Authentication Bypass by Capture-replay	24-03-2020	6.4	In Notifier Web Server (NWS) Version 3.50 and earlier, the Honeywell Fire Web Server's authentication may be bypassed by a capture-replay attack from a web browser. **CVE ID : CVE-2020-6972**	N/A	A-HON-NOTI-070420/184
win-pak					
N/A	24-03-2020	6.4	In Honeywell WIN-PAK 4.7.2, Web and prior versions, the affected product is vulnerable due to the usage of old jQuery libraries. **CVE ID : CVE-2020-6978**	N/A	A-HON-WIN--070420/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-03-2020	5.8	In Honeywell WIN-PAK 4.7.2, Web and prior versions, the header injection vulnerability has been identified, which may allow remote code execution. **CVE ID : CVE-2020-6982**	N/A	A-HON-WIN--070420/186
Cross-Site Request Forgery (CSRF)	24-03-2020	6.8	In Honeywell WIN-PAK 4.7.2, Web and prior versions, the affected product is vulnerable to a cross-site request forgery, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2020-7005**	N/A	A-HON-WIN--070420/187
Horde					
groupware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-03-2020	6.5	This vulnerability allows remote attackers to execute local PHP files on affected installations of Horde Groupware Webmail Edition 5.2.22. Authentication is required to exploit this vulnerability. The specific flaw exists within edit.php. When parsing the params[template] parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this in conjunction with other vulnerabilities to execute	N/A	A-HOR-GROU-070420/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the www-data user. Was ZDI-CAN-10469. **CVE ID : CVE-2020-8865**		
Unrestricted Upload of File with Dangerous Type	23-03-2020	4	This vulnerability allows remote attackers to create arbitrary files on affected installations of Horde Groupware Webmail Edition 5.2.22. Authentication is required to exploit this vulnerability. The specific flaw exists within add.php. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the www-data user. Was ZDI-CAN-10125. **CVE ID : CVE-2020-8866**	N/A	A-HOR-GROU-070420/189
Huawei					
manageone					
Double Free	20-03-2020	2.1	There is a double free vulnerability in some Huawei products. A local attacker with low privilege may perform some operations to exploit the vulnerability. Due to doubly freeing memory, successful exploit may cause some service abnormal. Affected	N/A	A-HUA-MANA-070420/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product versions include:CampusInsight versions V100R019C00;ManageOne versions 6.5.RC2.B050. **CVE ID : CVE-2020-1862**		
campusinsight					
Double Free	20-03-2020	2.1	There is a double free vulnerability in some Huawei products. A local attacker with low privilege may perform some operations to exploit the vulnerability. Due to doubly freeing memory, successful exploit may cause some service abnormal. Affected product versions include:CampusInsight versions V100R019C00;ManageOne versions 6.5.RC2.B050. **CVE ID : CVE-2020-1862**	N/A	A-HUA-CAMP-070420/191
IBM					
tivoli_netcool\/omnibus					
Cross-Site Request Forgery (CSRF)	18-03-2020	4.3	IBM Tivoli Netcool/OMNIbus 8.1.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 174910. **CVE ID : CVE-2020-4199**	https://www.ibm.com/support/pages/node/5968048	A-IBM-TIVO-070420/192
datapower_gateway					

CVSS 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
Information Exposure	19-03-2020	4	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.8 could potentially disclose highly sensitive information to a privileged user due to improper access controls. IBM X-Force ID: 174956. **CVE ID : CVE-2020-4203**	https://www.ibm.com/support/pages/node/6090934	A-IBM-DATA-070420/193
Improper Authentication	19-03-2020	6.5	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.8 could allow an authenticated user to bypass security restrictions, and continue to access the server even after authentication certificates have been revolked. IBM X-Force ID: 174961. **CVE ID : CVE-2020-4205**	https://www.ibm.com/support/pages/node/6090886	A-IBM-DATA-070420/194
websphere_application_server					
Improper Privilege Management	26-03-2020	6	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. X-Force ID: 175984. **CVE ID : CVE-2020-4276**	https://www.ibm.com/support/pages/node/6118222	A-IBM-WEBS-070420/195
content_navigator					
Insufficient Session Expiration	24-03-2020	6.5	IBM Content Navigator 3.0CD does not invalidate session after logout which could allow an authenticated user to	https://www.ibm.com/support/pages/node/611	A-IBM-CONT-070420/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impersonate another user on the system. IBM X-Force ID: 175559. **CVE ID : CVE-2020-4253**	6020	
Information Exposure	24-03-2020	5	IBM Content Navigator 3.0CD could disclose sensitive information to an unauthenticated user which could be used to aid in further attacks against the system. IBM X-Force ID: 177080. **CVE ID : CVE-2020-4309**	https://www.ibm.com/support/pages/node/6116032	A-IBM-CONT-070420/197
it-novum					
openitcockpit					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-03-2020	10	openITCOCKPIT before 3.7.3 has a web-based terminal that allows attackers to execute arbitrary OS commands via shell metacharacters that are mishandled on an su command line in app/Lib/SudoMessageInterface.php. **CVE ID : CVE-2020-10789**	https://openitcockpit.io/2020/2020/03/23/openitcockpit-3-7-3-released/	A-IT--OPEN-070420/198
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	3.5	openITCOCKPIT before 3.7.3 has unnecessary files (such as Lodash files) under the web root, which leads to XSS. **CVE ID : CVE-2020-10790**	https://openitcockpit.io/2020/2020/03/23/openitcockpit-3-7-3-released/	A-IT--OPEN-070420/199
Server-Side Request Forgery	25-03-2020	4	app/Plugin/GrafanaModule/Controller/GrafanaConfigurationController.php in	https://openitcockpit.io/2020/2020/	A-IT--OPEN-070420/200

CVSS 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
(SSRF)			openITCOCKPIT before 3.7.3 allows remote authenticated users to trigger outbound TCP requests (aka SSRF) via the Test Connection feature (aka testGrafanaConnection) of the Grafana Module. **CVE ID : CVE-2020-10791**	03/23/openitcockpit-3-7-3-released/	
Incorrect Default Permissions	20-03-2020	5	openITCOCKPIT through 3.7.2 allows remote attackers to configure the self::DEVELOPMENT or self::STAGING option by placing a hostname containing "dev" or "staging" in the HTTP Host header. **CVE ID : CVE-2020-10792**	https://openitcockpit.io/2020/2020/03/23/openitcockpit-3-7-3-released/	A-IT--OPEN-070420/201
Jenkins					
openshift_pipeline					
Improper Input Validation	25-03-2020	6.5	Jenkins OpenShift Pipeline Plugin 1.0.56 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability. **CVE ID : CVE-2020-2167**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1739	A-JEN-OPEN-070420/202
azure_container_service					
Improper Input Validation	25-03-2020	6.5	Jenkins Azure Container Service Plugin 1.0.1 and earlier does not configure its YAML parser to prevent	https://jenkins.io/security/advisory/2020-03-	A-JEN-AZUR-070420/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the instantiation of arbitrary types, resulting in a remote code execution vulnerability. **CVE ID : CVE-2020-2168**	25/#SECURITY-1732	
queue_cleanup					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	4.3	A form validation endpoint in Jenkins Queue cleanup Plugin 1.3 and earlier does not properly escape a query parameter displayed in an error message, resulting in a reflected XSS vulnerability. **CVE ID : CVE-2020-2169**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1724	A-JEN-QUEU-070420/204
jenkins					
Cross-Site Request Forgery (CSRF)	25-03-2020	6.8	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier uses different representations of request URL paths, which allows attackers to craft URLs that allow bypassing CSRF protection of any target URL. **CVE ID : CVE-2020-2160**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1774	A-JEN-JENK-070420/205
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	3.5	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not properly escape node labels that are shown in the form validation for label expressions on job configuration pages, resulting in a stored XSS vulnerability exploitable by users able to define node labels. **CVE ID : CVE-2020-2161**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1781	A-JEN-JENK-070420/206

CVSS 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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	3.5	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not set Content-Security-Policy headers for files uploaded as file parameters to a build, resulting in a stored XSS vulnerability. **CVE ID : CVE-2020-2162**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1793	A-JEN-JENK-070420/207
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	3.5	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier improperly processes HTML content of list view column headers, resulting in a stored XSS vulnerability exploitable by users able to control column headers. **CVE ID : CVE-2020-2163**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1796	A-JEN-JENK-070420/208
pipeline					
Improper Input Validation	25-03-2020	6.5	Jenkins Pipeline: AWS Steps Plugin 1.40 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability. **CVE ID : CVE-2020-2166**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1741	A-JEN-PIPE-070420/209
rapiddeploy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	3.5	Jenkins RapidDeploy Plugin 4.2 and earlier does not escape package names in the table of packages obtained from a remote server, resulting in a stored XSS vulnerability. **CVE ID : CVE-2020-2170**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1676	A-JEN-RAPI-070420/210

CVSS 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
Improper Restriction of XML External Entity Reference ('XXE')	25-03-2020	6.5	Jenkins RapidDeploy Plugin 4.2 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2171**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1677	A-JEN-RAPI-070420/211
Jfrog					
artifactory					
Insufficiently Protected Credentials	25-03-2020	4	Jenkins Artifactory Plugin 3.5.0 and earlier stores its Artifactory server password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system. **CVE ID : CVE-2020-2164**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1542%20(1)	A-JFR-ARTI-070420/212
Insufficiently Protected Credentials	25-03-2020	5	Jenkins Artifactory Plugin 3.6.0 and earlier transmits configured passwords in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2020-2165**	https://jenkins.io/security/advisory/2020-03-25/#SECURITY-1542%20(2)	A-JFR-ARTI-070420/213
Joomla					
joomla\!					
Exposure of Resource to Wrong Sphere	16-03-2020	5	An issue was discovered in Joomla! before 3.9.16. Various actions in com_templates lack the required ACL checks, leading to various potential attack vectors. **CVE ID : CVE-2020-**	N/A	A-JOO-JOOM-070420/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10238		
Missing Authorization	16-03-2020	6.5	An issue was discovered in Joomla! before 3.9.16. Incorrect Access Control in the SQL fieldtype of com_fields allows access for non-superadmin users. **CVE ID : CVE-2020-10239**	N/A	A-JOO-JOOM-070420/215
Improper Input Validation	16-03-2020	5	An issue was discovered in Joomla! before 3.9.16. Missing length checks in the user table can lead to the creation of users with duplicate usernames and/or email addresses. **CVE ID : CVE-2020-10240**	N/A	A-JOO-JOOM-070420/216
Cross-Site Request Forgery (CSRF)	16-03-2020	6.8	An issue was discovered in Joomla! before 3.9.16. Missing token checks in the image actions of com_templates lead to CSRF. **CVE ID : CVE-2020-10241**	N/A	A-JOO-JOOM-070420/217
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-03-2020	4.3	An issue was discovered in Joomla! before 3.9.16. Inadequate handling of CSS selectors in the Protostar and Beez3 JavaScript allows XSS attacks. **CVE ID : CVE-2020-10242**	N/A	A-JOO-JOOM-070420/218
Improper Neutralization of Special	16-03-2020	7.5	An issue was discovered in Joomla! before 3.9.16. The lack of type casting of a	N/A	A-JOO-JOOM-070420/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			variable in a SQL statement leads to a SQL injection vulnerability in the Featured Articles frontend menutype. **CVE ID : CVE-2020-10243**		
jsonparser_project					
jsonparser					
Loop with Unreachable Exit Condition ('Infinite Loop')	19-03-2020	5	The Library API in buger jsonparser through 2019-12-04 allows attackers to cause a denial of service (infinite loop) via a Delete call. **CVE ID : CVE-2020-10675**	N/A	A-JSO-JSON-070420/220
KDE					
okular					
Improper Input Validation	24-03-2020	6.8	KDE Okular before 1.10.0 allows code execution via an action link in a PDF document. **CVE ID : CVE-2020-9359**	https://invent.kde.org/kde/okular/-/commit/6a93a033b4f9248b3cd4d04689b8391df754e244, https://kde.org/info/security/advisory-20200312-1.txt	A-KDE-OKUL-070420/221
keijiban_tsumiki_project					
keijiban_tsumiki					
Improper Neutralization of Special	25-03-2020	10	Keijiban Tsumiki v1.15 allows remote attackers to execute arbitrary OS	N/A	A-KEI-KEIJ-070420/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			commands via unspecified vectors. **CVE ID : CVE-2020-5561**		
kiali					
kiali					
Use of Hard-coded Credentials	26-03-2020	7.5	A hard-coded cryptographic key vulnerability in the default configuration file was found in Kiali, all versions prior to 1.15.1. A remote attacker could abuse this flaw by creating their own JWT signed tokens and bypass Kiali authentication mechanisms, possibly gaining privileges to view and alter the Istio configuration. **CVE ID : CVE-2020-1764**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1764	A-KIA-KIAL-070420/223
Liferay					
liferay_portal					
Deserialization of Untrusted Data	20-03-2020	7.5	Deserialization of Untrusted Data in Liferay Portal prior to 7.2.1 CE GA2 allows remote attackers to execute arbitrary code via JSON web services (JSONWS). **CVE ID : CVE-2020-7961**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/117954271	A-LIF-LIFE-070420/224
lix_project					

CVSS 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
lix					
Authorization Bypass Through User-Controlled Key	21-03-2020	6.8	lix through 15.8.7 allows man-in-the-middle attackers to execute arbitrary code by modifying the HTTP client-server data stream so that the Location header is associated with attacker-controlled executable content in the postDownload field. **CVE ID : CVE-2020-10800**	N/A	A-LIX-LIX-070420/225
logicaldoc					
logicaldoc					
Unrestricted Upload of File with Dangerous Type	18-03-2020	10	LogicalDoc before 8.3.3 could allow an attacker to upload arbitrary files, leading to command execution or retrieval of data from the database. LogicalDoc provides a functionality to add documents. Those documents could then be used for multiple tasks, such as version control, shared among users, applying tags, etc. This functionality could be abused by an unauthenticated attacker to upload an arbitrary file in a restricted folder. This would lead to the executions of malicious commands with root privileges.	N/A	A-LOG-LOGI-070420/226

CVSS 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
			CVE ID : CVE-2020-9423		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-03-2020	4	LogicalDoc before 8.3.3 allows SQL Injection. LogicalDoc populates the list of available documents by querying the database. This list could be filtered by modifying some of the parameters. Some of them are not properly sanitized which could allow an authenticated attacker to perform arbitrary queries to the database. **CVE ID : CVE-2020-10365**	N/A	A-LOG-LOGI-070420/227
mailform					
mailform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	4.3	Cross-site scripting vulnerability in mailform version 1.04 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2020-5552**	N/A	A-MAI-MAIL-070420/228
Improper Control of Generation of Code ('Code Injection')	25-03-2020	10	mailform version 1.04 allows remote attackers to execute arbitrary PHP code via unspecified vectors. **CVE ID : CVE-2020-5553**	N/A	A-MAI-MAIL-070420/229
Mcafee					
application_and_change_control					
Untrusted Search Path	26-03-2020	4.4	DLL Side Loading vulnerability in the installer for McAfee Application and Change	https://kc.mcafee.com/corporate/index?page=co	A-MCA-APPL-070420/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Control (MACC) prior to 8.3 allows local users to execute arbitrary code via execution from a compromised folder. **CVE ID : CVE-2020-7260**	ntent&id=SB10313	
network_security_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-03-2020	3.5	Cross site scripting vulnerability in McAfee Network Security Management (NSM) Prior to 9.1 update 6 Mar 2020 Update allows attackers to unspecified impact via unspecified vectors. **CVE ID : CVE-2020-7256**	https://kc.mcafee.com/corporate/index?page=content&id=SB10310	A-MCA-NETW-070420/231
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-03-2020	3.5	Cross site scripting vulnerability in McAfee Network Security Management (NSM) Prior to 9.1 update 6 Mar 2020 Update allows attackers to unspecified impact via unspecified vectors. **CVE ID : CVE-2020-7258**	https://kc.mcafee.com/corporate/index?page=content&id=SB10310	A-MCA-NETW-070420/232
Memcached					
memcached					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-03-2020	5	Memcached 1.6.x before 1.6.2 allows remote attackers to cause a denial of service (daemon crash) via a crafted binary protocol header to try_read_command_binary in memcached.c. **CVE ID : CVE-2020-10931**	N/A	A-MEM-MEMC-070420/233

CVSS 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
Microfocus					
vibe					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	3.5	A stored XSS vulnerability was discovered in Micro Focus Vibe, affecting all Vibe version prior to 4.0.7. The vulnerability could allows a remote attacker to craft and store malicious content into Vibe such that when the content is viewed by another user of the system, attacker controlled JavaScript will execute in the security context of the target user's browser. **CVE ID : CVE-2020-9520**	N/A	A-MIC-VIBE-070420/234
service_manager_automation					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-03-2020	6.5	An SQL injection vulnerability was discovered in Micro Focus Service Manager Automation (SMA), affecting versions 2019.08, 2019.05, 2019.02, 2018.08, 2018.05, 2018.02. The vulnerability could allow for the improper neutralization of special elements in SQL commands and may lead to the product being vulnerable to SQL injection. **CVE ID : CVE-2020-9521**	N/A	A-MIC-SERV-070420/235
service_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	16-03-2020	5	Login filter can access configuration files vulnerability in Micro Focus Service Manager (Web Tier), affecting versions 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow unauthorized access to configuration data. **CVE ID : CVE-2020-9518**	N/A	A-MIC-SERV-070420/236
Information Exposure	16-03-2020	5	HTTP methods reveled in Web services vulnerability in Micro Focus Service manager (server), affecting versions 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62, 9.63. The vulnerability could be exploited to allow exposure of configuration data. **CVE ID : CVE-2020-9519**	N/A	A-MIC-SERV-070420/237
Mitre					
caldera					
Missing Authentication for Critical Function	22-03-2020	5	auth_svc in Caldera before 2.6.5 allows authentication bypass (for REST API requests) via a forged "localhost" string in the HTTP Host header. **CVE ID : CVE-2020-10807**	N/A	A-MIT-CALD-070420/238
Mozilla					
firefox					
Use After Free	25-03-2020	6.8	When removing data about an origin whose tab	N/A	A-MOZ-FIRE-070420/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was recently closed, a use-after-free could occur in the Quota manager, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6805**		
Out-of-bounds Read	25-03-2020	6.8	By carefully crafting promise resolutions, it was possible to cause an out-of-bounds read off the end of an array resized during script execution. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6806**	N/A	A-MOZ-FIRE-070420/240
Use After Free	25-03-2020	6.8	When a device was changed while a stream was about to be destroyed, the <code>stream-reinit</code> task may have been executed after the stream was destroyed, causing a use-after-free and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR	N/A	A-MOZ-FIRE-070420/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< 68.6. **CVE ID : CVE-2020-6807**		
Authentication Bypass by Spoofing	25-03-2020	4.3	When a JavaScript URL (javascript:) is evaluated and the result is a string, this string is parsed to create an HTML document, which is then presented. Previously, this document's URL (as reported by the document.location property, for example) was the originating javascript: URL which could lead to spoofing attacks; it is now correctly the URL of the originating document. This vulnerability affects Firefox < 74. **CVE ID : CVE-2020-6808**	N/A	A-MOZ-FIRE-070420/242
Information Exposure	25-03-2020	5	When a Web Extension had the all-urls permission and made a fetch request with a mode set to 'same-origin', it was possible for the Web Extension to read local files. This vulnerability affects Firefox < 74. **CVE ID : CVE-2020-6809**	N/A	A-MOZ-FIRE-070420/243
Improper Neutralization of Special Elements in Output Used by a Downstream	25-03-2020	6.8	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as	N/A	A-MOZ-FIRE-070420/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			Curl' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6811**		
Information Exposure	25-03-2020	5	The first time AirPods are connected to an iPhone, they become named after the user's name by default (e.g. Jane Doe's AirPods.) Websites with camera or microphone permission are able to enumerate device names, disclosing the user's name. To resolve this issue, Firefox added a special case that renames devices containing the substring 'AirPods' to simply 'AirPods'. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6812**	N/A	A-MOZ-FIRE-070420/245
N/A	25-03-2020	5	When protecting CSS blocks with the nonce feature of Content Security Policy, the @import statement in the CSS block could allow an attacker to	N/A	A-MOZ-FIRE-070420/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inject arbitrary styles, bypassing the intent of the Content Security Policy. This vulnerability affects Firefox < 74. **CVE ID : CVE-2020-6813**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Mozilla developers reported memory safety bugs present in Firefox and Thunderbird 68.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6814**	N/A	A-MOZ-FIRE-070420/247
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Mozilla developers reported memory safety and script safety bugs present in Firefox 73. Some of these bugs showed evidence of memory corruption or escalation of privilege and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 74. **CVE ID : CVE-2020-6815**	N/A	A-MOZ-FIRE-070420/248
firefox_esr					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	25-03-2020	6.8	When removing data about an origin whose tab was recently closed, a use-after-free could occur in the Quota manager, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6805**	N/A	A-MOZ-FIRE-070420/249
Out-of-bounds Read	25-03-2020	6.8	By carefully crafting promise resolutions, it was possible to cause an out-of-bounds read off the end of an array resized during script execution. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6806**	N/A	A-MOZ-FIRE-070420/250
Use After Free	25-03-2020	6.8	When a device was changed while a stream was about to be destroyed, the <code>stream-reinit</code> task may have been executed after the stream was destroyed, causing a use-after-free and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6,	N/A	A-MOZ-FIRE-070420/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6807**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-03-2020	6.8	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as Curl' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6811**	N/A	A-MOZ-FIRE-070420/252
Information Exposure	25-03-2020	5	The first time AirPods are connected to an iPhone, they become named after the user's name by default (e.g. Jane Doe's AirPods.) Websites with camera or microphone permission are able to enumerate device names, disclosing the user's name. To resolve this issue, Firefox added a special case that renames devices containing the substring 'AirPods' to simply 'AirPods'. This vulnerability affects	N/A	A-MOZ-FIRE-070420/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6812**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Mozilla developers reported memory safety bugs present in Firefox and Thunderbird 68.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6814**	N/A	A-MOZ-FIRE-070420/254
thunderbird					
Use After Free	25-03-2020	6.8	When removing data about an origin whose tab was recently closed, a use-after-free could occur in the Quota manager, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6805**	N/A	A-MOZ-THUN-070420/255
Out-of-bounds Read	25-03-2020	6.8	By carefully crafting promise resolutions, it was possible to cause an	N/A	A-MOZ-THUN-070420/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds read off the end of an array resized during script execution. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6806**		
Use After Free	25-03-2020	6.8	When a device was changed while a stream was about to be destroyed, the <code>stream-reinit</code> task may have been executed after the stream was destroyed, causing a use-after-free and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6807**	N/A	A-MOZ-THUN-070420/257
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-03-2020	6.8	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as Curl' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary	N/A	A-MOZ-THUN-070420/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command execution. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6811**		
Information Exposure	25-03-2020	5	The first time AirPods are connected to an iPhone, they become named after the user's name by default (e.g. Jane Doe's AirPods.) Websites with camera or microphone permission are able to enumerate device names, disclosing the user's name. To resolve this issue, Firefox added a special case that renames devices containing the substring 'AirPods' to simply 'AirPods'. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6812**	N/A	A-MOZ-THUN-070420/259
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Mozilla developers reported memory safety bugs present in Firefox and Thunderbird 68.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary	N/A	A-MOZ-THUN-070420/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6. **CVE ID : CVE-2020-6814**		
bleach					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-03-2020	4.3	In Mozilla Bleach before 3.11, a mutation XSS affects users calling bleach.clean with noscript and a raw tag in the allowed/whitelisted tags option. **CVE ID : CVE-2020-6802**	N/A	A-MOZ-BLEA-070420/261
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-03-2020	4.3	In Mozilla Bleach before 3.12, a mutation XSS in bleach.clean when RCDATA and either svg or math tags are whitelisted and the keyword argument strip=False. **CVE ID : CVE-2020-6816**	N/A	A-MOZ-BLEA-070420/262
Nagios					
nagios_xi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-03-2020	3.5	Nagios XI 5.6.11 allows XSS via the includes/components/ldap_ad_integration/ username parameter. **CVE ID : CVE-2020-10819**	N/A	A-NAG-NAGI-070420/263
Improper Neutralization of Input During Web Page	22-03-2020	3.5	Nagios XI 5.6.11 allows XSS via the includes/components/ldap_ad_integration/ password parameter.	N/A	A-NAG-NAGI-070420/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2020-10820**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-03-2020	3.5	Nagios XI 5.6.11 allows XSS via the account/main.php theme parameter. **CVE ID : CVE-2020-10821**	N/A	A-NAG-NAGI-070420/265
remote_plug_in_executor					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-03-2020	6.8	Nagios NRPE 3.2.1 has Insufficient Filtering because, for example, nasty_metachars interprets \n as the character \ and the character n (not as the \n newline sequence). This can cause command injection. **CVE ID : CVE-2020-6581**	N/A	A-NAG-REMO-070420/266
Out-of-bounds Write	16-03-2020	5	Nagios NRPE 3.2.1 has a Heap-Based Buffer Overflow, as demonstrated by interpretation of a small negative number as a large positive number during a bzero call. **CVE ID : CVE-2020-6582**	N/A	A-NAG-REMO-070420/267
nagios					
Improper Privilege Management	16-03-2020	4	Nagios Log Server 2.1.3 has Incorrect Access Control. **CVE ID : CVE-2020-6584**	N/A	A-NAG-NAGI-070420/268
Cross-Site	16-03-2020	6.8	Nagios Log Server 2.1.3	N/A	A-NAG-NAGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			has CSRF. **CVE ID : CVE-2020-6585**		070420/269
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-03-2020	3.5	Nagios Log Server 2.1.3 allows XSS by visiting /profile and entering a crafted name field that is mishandled on the /admin/users page. Any malicious user with limited access can store an XSS payload in his Name. When any admin views this, the XSS is triggered. **CVE ID : CVE-2020-6586**	N/A	A-NAG-NAGI-070420/270
Naver					
cloud_explorer					
Externally Controlled Reference to a Resource in Another Sphere	23-03-2020	7.5	Naver Cloud Explorer before 2.2.2.11 allows the attacker can move a local file in any path on the filesystem as a system privilege through its named pipe. **CVE ID : CVE-2020-9752**	https://cve.naver.com/detail/cve-2020-9752	A-NAV-CLOU-070420/271
Nextcloud					
nextcloud_server					
Server-Side Request Forgery (SSRF)	20-03-2020	4	A missing check for IPv4 nested inside IPv6 in Nextcloud server < 17.0.1, < 16.0.7, and < 15.0.14 allowed a Server-Side Request Forgery (SSRF) vulnerability when subscribing to a malicious calendar URL. **CVE ID : CVE-2020-8138**	https://nextcloud.com/security/advisory/?id=NC-SA-2020-014	A-NEX-NEXT-070420/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	20-03-2020	4	A missing access control check in Nextcloud Server < 18.0.1, < 17.0.4, and < 16.0.9 causes hide-download shares to be downloadable when appending /download to the URL. **CVE ID : CVE-2020-8139**	https://nextcloud.com/security/advisory/?id=NC-SA-2020-015	A-NEX-NEXT-070420/273
nextcloud					
Improper Control of Generation of Code ('Code Injection')	20-03-2020	4.6	A code injection in Nextcloud Desktop Client 2.6.2 for macOS allowed to load arbitrary code when starting the client with DYLD_INSERT_LIBRARIES set in the environment. **CVE ID : CVE-2020-8140**	https://nextcloud.com/security/advisory/?id=NC-SA-2020-016	A-NEX-NEXT-070420/274
octopus					
octopus_deploy					
Improper Privilege Management	19-03-2020	6.5	In Octopus Deploy before 2020.1.5, for customers running on-premises Active Directory linked to their Octopus server, an authenticated user can leverage a bug to escalate privileges. **CVE ID : CVE-2020-10678**	N/A	A-OCT-OCTO-070420/275
Opencart					
opencart					
Improper Neutralization of Input During Web Page Generation	17-03-2020	3.5	OpenCart 3.0.3.2 allows remote authenticated users to conduct XSS attacks via a crafted filename in the users'	N/A	A-OPE-OPEN-070420/276

CVSS 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
('Cross-site Scripting')			image upload section. **CVE ID : CVE-2020-10596**		
openwrt					
lede					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-03-2020	6.8	An issue was discovered in OpenWrt 18.06.0 to 18.06.6 and 19.07.0, and LEDE 17.01.0 to 17.01.7. A bug in the fork of the opkg package manager before 2020-01-25 prevents correct parsing of embedded checksums in the signed repository index, allowing a man-in-the-middle attacker to inject arbitrary package payloads (which are installed without verification). **CVE ID : CVE-2020-7982**	https://openwrt.org/advisory/2020-01-31-1	A-OPE-LEDE-070420/277
luci					
Information Exposure	23-03-2020	5	** DISPUTED ** In OpenWrt LuCI git-20.x, remote unauthenticated attackers can retrieve the list of installed packages and services. NOTE: the vendor disputes the significance of this report because, for instances reachable by an unauthenticated actor, the same information is available in other (more complex) ways, and there is no plan to restrict the information further.	N/A	A-OPE-LUCI-070420/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10871		
openwrt					
Out-of-bounds Write	16-03-2020	5	libubox in OpenWrt before 18.06.7 and 19.x before 19.07.1 has a tagged binary data JSON serialization vulnerability that may cause a stack based buffer overflow. **CVE ID : CVE-2020-7248**	https://openwrt.org/advisory/2020-01-31-2	A-OPE-OPEN-070420/279
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-03-2020	6.8	An issue was discovered in OpenWrt 18.06.0 to 18.06.6 and 19.07.0, and LEDE 17.01.0 to 17.01.7. A bug in the fork of the opkg package manager before 2020-01-25 prevents correct parsing of embedded checksums in the signed repository index, allowing a man-in-the-middle attacker to inject arbitrary package payloads (which are installed without verification). **CVE ID : CVE-2020-7982**	https://openwrt.org/advisory/2020-01-31-1	A-OPE-OPEN-070420/280
Parallels					
parallels_desktop					
Improper Privilege Management	23-03-2020	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute high-privileged code on the target guest system in	N/A	A-PAR-PARA-070420/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			order to exploit this vulnerability. The specific flaw exists within the xHCI component. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-10031. **CVE ID : CVE-2020-8873**		
Integer Overflow or Wraparound	23-03-2020	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the xHCI component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-10032. **CVE ID : CVE-2020-8874**	N/A	A-PAR-PARA-070420/282
Out-of-	23-03-2020	7.2	This vulnerability allows	N/A	A-PAR-PARA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the IOCTL handler. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-10028. **CVE ID : CVE-2020-8875**		070420/283
Out-of-bounds Read	23-03-2020	2.1	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the IOCTL handler. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an	N/A	A-PAR-PARA-070420/284

CVSS 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
			allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-10029. **CVE ID : CVE-2020-8876**		
Out-of-bounds Write	23-03-2020	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.0-47107 . An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the VGA virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-9403. **CVE ID : CVE-2020-8871**	N/A	A-PAR-PARA-070420/285
Out-of-bounds Read	23-03-2020	2.1	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.1-47117. An attacker must first obtain the ability to	N/A	A-PAR-PARA-070420/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the xHCI component. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the hypervisor. Was ZDI-CAN-9428. **CVE ID : CVE-2020-8872**		
perlspeak_project					
perlspeak					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-03-2020	7.5	PerlSpeak through 2.01 allows attackers to execute arbitrary OS commands, as demonstrated by use of system and 2-argument open. **CVE ID : CVE-2020-10674**	N/A	A-PER-PERL-070420/287
Phpmyadmin					
phpmyadmin					
Improper Neutralization of Special Elements used in an SQL Command	22-03-2020	6	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability has been discovered where certain parameters are not properly escaped when	N/A	A-PHP-PHPM-070420/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			generating certain queries for search actions in libraries/classes/Controllers/Table/TableSearchController.php. An attacker can generate a crafted database or table name. The attack can be performed if a user attempts certain search operations on the malicious database or table. **CVE ID : CVE-2020-10802**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-03-2020	3.5	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was discovered where malicious code could be used to trigger an XSS attack through retrieving and displaying results (in tbl_get_field.php and libraries/classes/Display/Results.php). The attacker must be able to insert crafted data into certain database tables, which when retrieved (for instance, through the Browse tab) can trigger the XSS attack. **CVE ID : CVE-2020-10803**	N/A	A-PHP-PHPM-070420/289
Improper Neutralization of Special Elements	22-03-2020	6	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was found in	N/A	A-PHP-PHPM-070420/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			retrieval of the current username (in libraries/classes/Server/Privileges.php and libraries/classes/UserPassword.php). A malicious user with access to the server could create a crafted username, and then trick the victim into performing specific actions with that user account (such as editing its privileges). **CVE ID : CVE-2020-10804**		
Piwigo					
piwigo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-03-2020	3.5	Piwigo 2.10.1 has stored XSS via the file parameter in a /ws.php request because of the pwg.images.setInfo function. **CVE ID : CVE-2020-9467**	https://github.com/Piwigo/Piwigo/issues/1168	A-PIW-PIWI-070420/291
Postgresql					
postgresql					
Missing Authorization	17-03-2020	3.5	A flaw was found in PostgreSQL's "ALTER ... DEPENDS ON EXTENSION", where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1720	A-POS-POST-070420/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2, before 11.7, before 10.12 and before 9.6.17. **CVE ID : CVE-2020-1720**		
Prestashop					
faceted_search_module					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	3.5	PrestaShop module ps_facetedsearch versions before 3.5.0 has a reflected XSS with `url_name` parameter. The problem is fixed in 3.5.0 **CVE ID : CVE-2020-5277**	https://github.com/PrestaShop/ps_facetedsearch/security/advisories/GHSA-mmmv-m5q9-g3cm	A-PRE-FACE-070420/293
psi					
electronic_logbook					
NULL Pointer Dereference	23-03-2020	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of ELOG Electronic Logbook 3.1.4-283534d. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of HTTP parameters. A crafted request can trigger the dereference of a null pointer. An attacker can leverage this vulnerability to create a denial-of-service condition. Was ZDI-CAN-10115.	N/A	A-PSI-ELEC-070420/294

CVSS 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
			CVE ID : CVE-2020-8859		
pyup					
safety					
N/A	23-03-2020	1.9	The command-line "safety" package for Python has a potential security issue. There are two Python characteristics that allow malicious code to “poison-pill” command-line Safety package detection routines by disguising, or obfuscating, other malicious or non-secure packages. This vulnerability is considered to be of low severity because the attack makes use of an existing Python condition, not the Safety tool itself. This can happen if: You are running Safety in a Python environment that you don’t trust. You are running Safety from the same Python environment where you have your dependencies installed. Dependency packages are being installed arbitrarily or without proper verification. Users can mitigate this issue by doing any of the following: Perform a static analysis by installing Docker and running the Safety Docker image: $ docker run --rm -it pyupio/safety check -r	https://github.com/akoumjian/python-safety-vuln, https://github.com/pyupio/safety/security/advisories/GHSA-7q25-qrjw-6fg2, https://pyup.io/posts/patched-vulnerability/	A-PYU-SAFE-070420/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requirements.txt Run Safety against a static dependencies list, such as the requirements.txt file, in a separate, clean Python environment. Run Safety from a Continuous Integration pipeline. Use PyUp.io, which runs Safety in a controlled environment and checks Python for dependencies without any need to install them. Use PyUp's Online Requirements Checker. **CVE ID : CVE-2020-5252**		
Quest					
foglight_evolve					
Use of Hard-coded Credentials	23-03-2020	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight Evolve 9.0.0. Authentication is not required to exploit this vulnerability. The specific flaw exists within the __service__ user account. The product contains a hard-coded password for this account. An attacker can leverage this vulnerability to execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-9553. **CVE ID : CVE-2020-8868**	N/A	A-QUE-FOGL-070420/296
rconfig					
rconfig					

CVSS 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
Insufficiently Protected Credentials	20-03-2020	5	An issue was discovered in includes/head.inc.php in rConfig before 3.9.4. An unauthenticated attacker can retrieve saved cleartext credentials via a GET request to settings.php. Because the application was not exiting after a redirect is applied, the rest of the page still executed, resulting in the disclosure of cleartext credentials in the response. **CVE ID : CVE-2020-9425**	https://github.com/rconfig/rconfig/commit/20f4e3d87e84663d922b937842fddd9af1b68dd9	A-RCO-RCON-070420/297
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-03-2020	7.5	rConfig before 3.9.5 allows command injection by sending a crafted GET request to lib/crud/search.crud.php since the nodeId parameter is passed directly to the exec function without being escaped. **CVE ID : CVE-2020-10879**	N/A	A-RCO-RCON-070420/298
r-consortium					
rmysql					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-03-2020	7.5	RMySQL through 0.10.19 allows SQL Injection. **CVE ID : CVE-2020-10380**	https://github.com/r-dbi/RMySQL/blob/master/NEWS.md	A-R-C-RMYS-070420/299

CVSS 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
Redhat					
ansible_engine					
Information Exposure Through Log Files	16-03-2020	2.1	A security flaw was found in Ansible Engine, all Ansible 2.7.x versions prior to 2.7.17, all Ansible 2.8.x versions prior to 2.8.11 and all Ansible 2.9.x versions prior to 2.9.7, when managing kubernetes using the k8s module. Sensitive parameters such as passwords and tokens are passed to kubectl from the command line, not using an environment variable or an input configuration file. This will disclose passwords and tokens from process list and no_log directive from debug module would not have any effect making these secrets being disclosed on stdout and log files. **CVE ID : CVE-2020-1753**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1753, https://github.com/ansible-collections/kubernetes/pull/51	A-RED-ANSI-070420/300
certificate_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-03-2020	3.5	A flaw was found in the all pki-core 10.x.x versions, where Token Processing Service (TPS) where it did not properly sanitize Profile IDs, enabling a Stored Cross-Site Scripting (XSS) vulnerability when the profile ID is printed. An attacker with sufficient permissions could trick an	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1696	A-RED-CERT-070420/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated victim into executing a specially crafted Javascript code. **CVE ID : CVE-2020-1696**		
template_service_broker_operator					
Improper Privilege Management	19-03-2020	4.4	A vulnerability was found in openshift/template-service-broker-operator in all 4.x.x versions prior to 4.3.0, where an insecure modification vulnerability in the /etc/passwd file was found in the openshift/template-service-broker-operator. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges. **CVE ID : CVE-2020-1705**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1705	A-RED-TEMP-070420/302
decision_manager					
Missing Authorization	17-03-2020	3.5	A flaw was found in PostgreSQL's "ALTER ... DEPENDS ON EXTENSION", where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2, before 11.7, before 10.12	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1720	A-RED-DECI-070420/303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and before 9.6.17. **CVE ID : CVE-2020-1720**		
software_collections					
Missing Authorization	17-03-2020	3.5	A flaw was found in PostgreSQL's "ALTER ... DEPENDS ON EXTENSION", where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2, before 11.7, before 10.12 and before 9.6.17. **CVE ID : CVE-2020-1720**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1720	A-RED-SOFT-070420/304
keycloak					
Information Exposure	24-03-2020	5	A flaw was found in keycloak before version 9.0.1. When configuring an Conditional OTP Authentication Flow as a post login flow of an IDP, the failure login events for OTP are not being sent to the brute force protection event queue. So BruteForceProtector does not handle this events. **CVE ID : CVE-2020-1744**	https://access.redhat.com/security/cve/CVE-2020-1744, https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1744	A-RED-KEYC-070420/305
ansible					
Improper	16-03-2020	3.6	A flaw was found in the	https://bugz	A-RED-ANSI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			Ansible Engine when the fetch module is used. An attacker could intercept the module, inject a new path, and then choose a new destination path on the controller node. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1735**	illa.redhat.com/show_bug.cgi?id=CVE-2020-1735, https://github.com/ansible/ansible/issues/67793	070420/306
Incorrect Permission Assignment for Critical Resource	16-03-2020	2.1	A flaw was found in Ansible Engine when a file is moved using atomic_move primitive as the file mode cannot be specified. This sets the destination files world-readable if the destination file does not exist and if the file exists, the file could be changed to have less restrictive permissions before the move. This could lead to the disclosure of sensitive data. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1736**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1736, https://github.com/ansible/ansible/issues/67794	A-RED-ANSI-070420/307
Argument Injection or Modification	16-03-2020	4.4	A flaw was found in Ansible Engine when the module package or service is used and the parameter 'use' is not specified. If a previous task is executed with a malicious user, the module sent can be selected by the attacker	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1738, https://github.com/ansible/ansible/issues/6779	A-RED-ANSI-070420/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using the ansible facts file. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1738**	6	
Improper Control of Generation of Code ('Code Injection')	24-03-2020	3.6	A flaw was found in Ansible Engine, all versions 2.7.x, 2.8.x and 2.9.x prior to 2.7.17, 2.8.9 and 2.9.6 respectively, when using ansible_facts as a subkey of itself and promoting it to a variable when inject is enabled, overwriting the ansible_facts after the clean. An attacker could take advantage of this by altering the ansible_facts, such as ansible_hosts, users and any other key data which would lead into privilege escalation or code injection. **CVE ID : CVE-2020-10684**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10684	A-RED-ANSI-070420/309
Information Exposure	16-03-2020	1.9	A flaw was found in Ansible Engine when using Ansible Vault for editing encrypted files. When a user executes "ansible-vault edit", another user on the same computer can read the old and new secret, as it is created in a temporary file with mkstemp and the returned file descriptor is closed and the method write_data is called to write the	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1740, https://github.com/ansible/ansible/issues/67798	A-RED-ANSI-070420/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			existing secret in the file. This method will delete the file before recreating it insecurely. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1740**		
openstack					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-03-2020	3.6	A flaw was found in the Ansible Engine when the fetch module is used. An attacker could intercept the module, inject a new path, and then choose a new destination path on the controller node. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1735**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1735, https://github.com/ansible/ansible/issues/67793	A-RED-OPEN-070420/311
Incorrect Permission Assignment for Critical Resource	16-03-2020	2.1	A flaw was found in Ansible Engine when a file is moved using atomic_move primitive as the file mode cannot be specified. This sets the destination files world-readable if the destination file does not exist and if the file exists, the file could be changed to have less restrictive permissions before the move. This could lead to the disclosure of sensitive data. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1736, https://github.com/ansible/ansible/issues/67794	A-RED-OPEN-070420/312

CVSS 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
			vulnerable. **CVE ID : CVE-2020-1736**		
Argument Injection or Modification	16-03-2020	4.4	A flaw was found in Ansible Engine when the module package or service is used and the parameter 'use' is not specified. If a previous task is executed with a malicious user, the module sent can be selected by the attacker using the ansible facts file. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1738**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1738, https://github.com/ansible/ansible/issues/67796	A-RED-OPEN-070420/313
Improper Control of Generation of Code ('Code Injection')	24-03-2020	3.6	A flaw was found in Ansible Engine, all versions 2.7.x, 2.8.x and 2.9.x prior to 2.7.17, 2.8.9 and 2.9.6 respectively, when using ansible_facts as a subkey of itself and promoting it to a variable when inject is enabled, overwriting the ansible_facts after the clean. An attacker could take advantage of this by altering the ansible_facts, such as ansible_hosts, users and any other key data which would lead into privilege escalation or code injection. **CVE ID : CVE-2020-10684**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10684	A-RED-OPEN-070420/314
Information Exposure	16-03-2020	1.9	A flaw was found in Ansible Engine when using	https://bugzilla.redhat.co	A-RED-OPEN-070420/315

CVSS 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
			Ansible Vault for editing encrypted files. When a user executes "ansible-vault edit", another user on the same computer can read the old and new secret, as it is created in a temporary file with mkstemp and the returned file descriptor is closed and the method write_data is called to write the existing secret in the file. This method will delete the file before recreating it insecurely. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1740**	m/show_bug.cgi?id=CVE-2020-1740, https://github.com/ansible/ansible/issues/67798	
ansible_tower					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-03-2020	3.6	A flaw was found in the Ansible Engine when the fetch module is used. An attacker could intercept the module, inject a new path, and then choose a new destination path on the controller node. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1735**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1735, https://github.com/ansible/ansible/issues/67793	A-RED-ANSI-070420/316
Incorrect Permission Assignment for Critical Resource	16-03-2020	2.1	A flaw was found in Ansible Engine when a file is moved using atomic_move primitive as the file mode cannot be specified. This sets the destination files world-	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1736, https://github.com/ansi	A-RED-ANSI-070420/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			readable if the destination file does not exist and if the file exists, the file could be changed to have less restrictive permissions before the move. This could lead to the disclosure of sensitive data. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1736**	ble/ansible/issues/67794	
Argument Injection or Modification	16-03-2020	4.4	A flaw was found in Ansible Engine when the module package or service is used and the parameter 'use' is not specified. If a previous task is executed with a malicious user, the module sent can be selected by the attacker using the ansible facts file. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1738**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1738, https://github.com/ansible/ansible/issues/67796	A-RED-ANSI-070420/318
Improper Control of Generation of Code ('Code Injection')	24-03-2020	3.6	A flaw was found in Ansible Engine, all versions 2.7.x, 2.8.x and 2.9.x prior to 2.7.17, 2.8.9 and 2.9.6 respectively, when using ansible_facts as a subkey of itself and promoting it to a variable when inject is enabled, overwriting the ansible_facts after the clean. An attacker could take advantage of this by	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10684	A-RED-ANSI-070420/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			altering the ansible_facts, such as ansible_hosts, users and any other key data which would lead into privilege escalation or code injection. **CVE ID : CVE-2020-10684**		
Information Exposure	16-03-2020	1.9	A flaw was found in Ansible Engine when using Ansible Vault for editing encrypted files. When a user executes "ansible-vault edit", another user on the same computer can read the old and new secret, as it is created in a temporary file with mkstemp and the returned file descriptor is closed and the method write_data is called to write the existing secret in the file. This method will delete the file before recreating it insecurely. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1740**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1740, https://github.com/ansible/ansible/issues/67798	A-RED-ANSI-070420/320
Information Exposure Through Log Files	16-03-2020	2.1	A security flaw was found in Ansible Engine, all Ansible 2.7.x versions prior to 2.7.17, all Ansible 2.8.x versions prior to 2.8.11 and all Ansible 2.9.x versions prior to 2.9.7, when managing kubernetes using the k8s module. Sensitive	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1753, https://github.com/ansible-collections/kubernetes/p	A-RED-ANSI-070420/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameters such as passwords and tokens are passed to kubectl from the command line, not using an environment variable or an input configuration file. This will disclose passwords and tokens from process list and no_log directive from debug module would not have any effect making these secrets being disclosed on stdout and log files. **CVE ID : CVE-2020-1753**	ull/51	
openshift					
Improper Privilege Management	20-03-2020	4.4	A vulnerability was found in all openshift/postgresql-apb 4.x.x versions prior to 4.3.0, where an insecure modification vulnerability in the /etc/passwd file was found in the container openshift/postgresql-apb. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges. **CVE ID : CVE-2020-1707**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1707	A-RED-OPEN-070420/322
Improper Privilege Management	20-03-2020	4.6	A vulnerability was found in all openshift/mediawiki 4.x.x versions prior to 4.3.0, where an insecure modification vulnerability in the /etc/passwd file was found in the openshift/mediawiki. An	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1709	A-RED-OPEN-070420/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges. **CVE ID : CVE-2020-1709**		
openshift_service_mesh					
Use of Hard-coded Credentials	26-03-2020	7.5	A hard-coded cryptographic key vulnerability in the default configuration file was found in Kiali, all versions prior to 1.15.1. A remote attacker could abuse this flaw by creating their own JWT signed tokens and bypass Kiali authentication mechanisms, possibly gaining privileges to view and alter the Istio configuration. **CVE ID : CVE-2020-1764**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1764	A-RED-OPEN-070420/324
cloudforms_management_engine					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-03-2020	3.6	A flaw was found in the Ansible Engine when the fetch module is used. An attacker could intercept the module, inject a new path, and then choose a new destination path on the controller node. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1735**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1735, https://github.com/ansible/ansible/issues/67793	A-RED-CLOU-070420/325
Incorrect Permission Assignment	16-03-2020	2.1	A flaw was found in Ansible Engine when a file is moved using	https://bugzilla.redhat.com/show_bug	A-RED-CLOU-070420/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
for Critical Resource			atomic_move primitive as the file mode cannot be specified. This sets the destination files world-readable if the destination file does not exist and if the file exists, the file could be changed to have less restrictive permissions before the move. This could lead to the disclosure of sensitive data. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1736**	.cgi?id=CVE-2020-1736, https://github.com/ansible/ansible/issues/67794	
Argument Injection or Modification	16-03-2020	4.4	A flaw was found in Ansible Engine when the module package or service is used and the parameter 'use' is not specified. If a previous task is executed with a malicious user, the module sent can be selected by the attacker using the ansible facts file. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1738**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1738, https://github.com/ansible/ansible/issues/67796	A-RED-CLOU-070420/327
Information Exposure	16-03-2020	1.9	A flaw was found in Ansible Engine when using Ansible Vault for editing encrypted files. When a user executes "ansible-vault edit", another user on the same computer can read the old and new secret, as it is created in a	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1740, https://github.com/ansible/ansible/issues/6779	A-RED-CLOU-070420/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			temporary file with mkstemp and the returned file descriptor is closed and the method write_data is called to write the existing secret in the file. This method will delete the file before recreating it insecurely. All versions in 2.7.x, 2.8.x and 2.9.x branches are believed to be vulnerable. **CVE ID : CVE-2020-1740**	8	
Rockwellautomation					
factorytalk_services_platform					
Deserialization of Untrusted Data	23-03-2020	10	In Rockwell Automation all versions of FactoryTalk Diagnostics software, a subsystem of the FactoryTalk Services Platform, FactoryTalk Diagnostics exposes a .NET Remoting endpoint via RNADiagnosticsSrv.exe at TCPtcp/8082, which can insecurely deserialize untrusted data. **CVE ID : CVE-2020-6967**	N/A	A-ROC-FACT-070420/329
rslogix_500					
Cleartext Storage of Sensitive Information	16-03-2020	2.1	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP)	N/A	A-ROC-RSLO-070420/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext. **CVE ID : CVE-2020-6980**		
Use of a Broken or Risky Cryptographic Algorithm	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic function utilized to protect the password in MicroLogix is discoverable. **CVE ID : CVE-2020-6984**	N/A	A-ROC-RSLO-070420/331
Improper Authentication	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the	N/A	A-ROC-RSLO-070420/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials. **CVE ID : CVE-2020-6988**		
Use of Hard-coded Credentials	16-03-2020	10	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller. **CVE ID : CVE-2020-6990**	N/A	A-ROC-RSLO-070420/333
Rubyonrails					
actionview					
Improper Neutralization of Input During Web Page Generation	19-03-2020	3.5	In ActionView before versions 6.0.2.2 and 5.2.4.2, there is a possible XSS vulnerability in ActionView's JavaScript literal escape helpers.	https://github.com/rails/rails/security/advisories/GHSA-65cv-r6x7-	A-RUB-ACTI-070420/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Views that use the `j` or `escape_javascript` methods may be susceptible to XSS attacks. The issue is fixed in versions 6.0.2.2 and 5.2.4.2. **CVE ID : CVE-2020-5267**	79hv	
S9Y					
serendipity					
Unrestricted Upload of File with Dangerous Type	25-03-2020	7.5	Serendipity before 2.3.4 on Windows allows remote attackers to execute arbitrary code because the filename of a renamed file may end with a dot. This file may then be renamed to have a .php filename. **CVE ID : CVE-2020-10964**	N/A	A-S9Y-SERE-070420/335
salesagility					
suitecrm					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-03-2020	7.5	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue 1 of 4). **CVE ID : CVE-2020-8783**	https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_23, https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_11	A-SAL-SUIT-070420/336
Improper Neutralization of Special Elements	16-03-2020	7.5	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue	https://docs.suitecrm.com/admin/releases/7.10.	A-SAL-SUIT-070420/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			2 of 4). **CVE ID : CVE-2020-8784**	x/#_7_10_23, https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_11	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-03-2020	7.5	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue 3 of 4). **CVE ID : CVE-2020-8785**	https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_23, https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_11	A-SAL-SUIT-070420/338
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-03-2020	7.5	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow SQL Injection (issue 4 of 4). **CVE ID : CVE-2020-8786**	https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_23, https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_11	A-SAL-SUIT-070420/339
Improper Input Validation	16-03-2020	5	SuiteCRM 7.10.x versions prior to 7.10.23 and 7.11.x versions prior to 7.11.11 allow for an invalid Bean ID to be submitted. **CVE ID : CVE-2020-8787**	https://docs.suitecrm.com/admin/releases/7.10.x/#_7_10_23, https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_11	A-SAL-SUIT-070420/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Schneider-electric					
pmepxm0100_prosoft_configurator					
Uncontrolled Search Path Element	23-03-2020	4.4	A CWE-427: Uncontrolled Search Path Element vulnerability exists in ProSoft Configurator (v1.002 and prior), for the PMEPXM0100 (H) module, which could cause the execution of untrusted code when using double click to open a project file which may trigger execution of a malicious DLL. **CVE ID : CVE-2020-7474**	N/A	A-SCH-PMEP-070420/341
ecostruxure_control_expert					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-03-2020	7.5	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), reflective DLL, vulnerability exists in EcoStruxure Control Expert (all versions prior to 14.1 Hot Fix), Unity Pro (all versions), Modicon M340 (all versions prior to V3.20), Modicon M580 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller. **CVE ID : CVE-2020-7475**	N/A	A-SCH-ECOS-070420/342
unity_pro					
Improper Neutralizatio	23-03-2020	7.5	A CWE-74: Improper Neutralization of Special	N/A	A-SCH-UNIT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			Elements in Output Used by a Downstream Component ('Injection'), reflective DLL, vulnerability exists in EcoStruxure Control Expert (all versions prior to 14.1 Hot Fix), Unity Pro (all versions), Modicon M340 (all versions prior to V3.20), Modicon M580 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller. **CVE ID : CVE-2020-7475**		070420/343
ulti_zigbee_installation_toolkit					
Untrusted Search Path	23-03-2020	4.4	A CWE-426: Untrusted Search Path vulnerability exists in ZigBee Installation Kit (Versions prior to 1.0.1), which could cause execution of malicious code when a malicious file is put in the search path. **CVE ID : CVE-2020-7476**	N/A	A-SCH-ULTI-070420/344
interactive_graphical_scada_system					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-03-2020	5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory exists in IGSS (Versions 14 and prior using the service: IGSSupdate), which could allow a remote unauthenticated attacker to read arbitrary files from the IGSS server	N/A	A-SCH-INTE-070420/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC on an unrestricted or shared network when the IGSS Update Service is enabled. **CVE ID : CVE-2020-7478**		
Missing Authentication for Critical Function	23-03-2020	4.6	A CWE-306: Missing Authentication for Critical Function vulnerability exists in IGSS (Versions 14 and prior using the service: IGSSupdate), which could allow a local user to execute processes that otherwise require escalation privileges when sending local network commands to the IGSS Update Service. **CVE ID : CVE-2020-7479**	N/A	A-SCH-INTE-070420/346
shihonkanri_plus_goout_project					
shihonkanri_plus_goout					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-03-2020	6.4	Directory traversal vulnerability in Shihonkanri Plus GOOUT Ver1.5.8 and Ver2.2.10 allows remote attackers to read and write arbitrary files via unspecified vectors. **CVE ID : CVE-2020-5554**	N/A	A-SHI-SHIH-070420/347
Improper Input Validation	25-03-2020	6.4	Shihonkanri Plus GOOUT Ver1.5.8 and Ver2.2.10 allows remote attackers to read and write data of the files placed in the same directory where it is placed via unspecified vector due to the improper input validation	N/A	A-SHI-SHIH-070420/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2020-5555**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-03-2020	10	Shihonkanri Plus GOOUT Ver1.5.8 and Ver2.2.10 allows remote attackers to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2020-5556**	N/A	A-SHI-SHIH-070420/349
signotec					
signopad-api\/web					
Improper Input Validation	20-03-2020	4.3	An issue was discovered in signotec signoPAD-API/Web (formerly Websocket Pad Server) before 3.1.1 on Windows. It is possible to perform a Denial of Service attack because the implementation doesn't limit the parsing of nested JSON structures. If a victim visits an attacker-controlled website, this vulnerability can be exploited via WebSocket data with a deeply nested JSON array. **CVE ID : CVE-2020-9343**	N/A	A-SIG-SIGN-070420/350
Allocation of Resources Without Limits or Throttling	20-03-2020	4.3	An issue was discovered in signotec signoPAD-API/Web (formerly Websocket Pad Server) before 3.1.1 on Windows. It is possible to perform a Denial of Service attack because the application	N/A	A-SIG-SIGN-070420/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			doesn't limit the number of opened WebSocket sockets. If a victim visits an attacker-controlled website, this vulnerability can be exploited. **CVE ID : CVE-2020-9345**		
Simplesamlphp					
saml2					
Authentication Bypass by Capture-replay	25-03-2020	4.9	Saml2 Authentication services for ASP.NET (NuGet package Sustainsys.Saml2) greater than 2.0.0, and less than version 2.5.0 has a faulty implementation of Token Replay Detection. Token Replay Detection is an important defence in depth measure for Single Sign On solutions. The 2.5.0 version is patched. Note that version 1.0.1 is not affected. It has a correct Token Replay Implementation and is safe to use. Saml2 Authentication services for ASP.NET (NuGet package Sustainsys.Saml2) greater than 2.0.0, and less than version 2.5.0 have a faulty implementation of Token Replay Detection. Token Replay Detection is an important defense measure for Single Sign On solutions. The 2.5.0 version is patched. Note that version 1.0.1 and	https://github.com/Sustainsys/Saml2/security/advisories/GHSA-g6j2-ch25-5mmv	A-SIM-SAML-070420/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior versions are not affected. These versions have a correct Token Replay Implementation and are safe to use. **CVE ID : CVE-2020-5261**		
SUN					
ehrd					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-03-2020	4.3	Sunnet eHRD, a human training and development management system, contains vulnerability of Cross-Site Scripting (XSS), attackers can inject arbitrary command into the system and launch XSS attack. **CVE ID : CVE-2020-10509**	https://www.chtsecurity.com/news/30772cf1-2e7e-4afe-9282-b5a196b22e71	A-SUN-EHRD-070420/353
supsystic					
pricing_table_by_supsystic					
Incorrect Default Permissions	23-03-2020	7.5	An issue was discovered in the pricing-table-by-supsystic plugin before 1.8.2 for WordPress. Because there is no permission check on the ImportJSONTable, createFromTpl, and getJSONExportTable endpoints, unauthenticated users can retrieve pricing table information, create new tables, or import/modify a table. **CVE ID : CVE-2020-9392**	N/A	A-SUP-PRIC-070420/354
svglib_project					

CVSS 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
svglib					
Improper Restriction of XML External Entity Reference ('XXE')	20-03-2020	7.5	The svglib package through 0.9.3 for Python allows XXE attacks via an svg2rlg call. **CVE ID : CVE-2020-10799**	N/A	A-SVG-SVGL-070420/355
Telegram					
telegram					
Improper Authentication	24-03-2020	3.6	The Telegram application through 5.12 for Android, when Show Popup is enabled, might allow physically proximate attackers to bypass intended restrictions on message reading and message replying. This might be interpreted as a bypass of the passcode feature. **CVE ID : CVE-2020-10570**	N/A	A-TEL-TELE-070420/356
Tesla					
model_3_web_interface					
Improper Privilege Management	20-03-2020	7.1	The driving interface of Tesla Model 3 vehicles in any release before 2020.4.10 allows Denial of Service to occur due to improper process separation, which allows attackers to disable the speedometer, web browser, climate controls, turn signal visual and sounds, navigation, autopilot notifications,	N/A	A-TES-MODE-070420/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			along with other miscellaneous functions from the main screen. **CVE ID : CVE-2020-10558**		
thimpress					
learnpress					
Improper Privilege Management	16-03-2020	4	be_teacher in class-lp-admin-ajax.php in the LearnPress plugin 3.2.6.5 and earlier for WordPress allows any registered user to assign itself the teacher role via the wp-admin/admin-ajax.php?action=learnpress_be_teacher URI without any additional permission checks. Therefore, any user can change its role to an instructor/teacher and gain access to otherwise restricted data. **CVE ID : CVE-2020-7916**	https://wordpress.org/plugins/learnpress/#developers	A-THI-LEAR-070420/358
Torproject					
tor					
Uncontrolled Resource Consumption	23-03-2020	5	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (CPU consumption), aka TROVE-2020-002. **CVE ID : CVE-2020-10592**	N/A	A-TOR-TOR-070420/359
Improper Release of Memory	23-03-2020	5	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows	N/A	A-TOR-TOR-070420/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Before Removing Last Reference			remote attackers to cause a Denial of Service (memory leak), aka TROVE-2020-004. This occurs in circpad_setup_machine_on_circ because a circuit-padding machine can be negotiated twice on the same circuit. **CVE ID : CVE-2020-10593**		
Trendmicro					
apex_one					
N/A	18-03-2020	6.5	A migration tool component of Trend Micro Apex One (2019) and OfficeScan XG contains a vulnerability which could allow remote attackers to execute arbitrary code on affected installations (RCE). An attempted attack requires user authentication. **CVE ID : CVE-2020-8467**	N/A	A-TRE-APEX-070420/361
Download of Code Without Integrity Check	18-03-2020	6.5	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication. **CVE ID : CVE-2020-8468**	N/A	A-TRE-APEX-070420/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-03-2020	9.4	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not required to exploit this vulnerability. **CVE ID : CVE-2020-8470**	N/A	A-TRE-APEX-070420/363
Improper Input Validation	18-03-2020	10	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit this vulnerability. **CVE ID : CVE-2020-8598**	N/A	A-TRE-APEX-070420/364
Unrestricted Upload of File with Dangerous Type	18-03-2020	10	Trend Micro Apex One (2019) and OfficeScan XG server contain a vulnerable EXE file that could allow a remote attacker to write arbitrary data to an arbitrary path on affected installations and bypass ROOT login. Authentication is not required to exploit this	N/A	A-TRE-APEX-070420/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2020-8599**		
officescan					
N/A	18-03-2020	6.5	A migration tool component of Trend Micro Apex One (2019) and OfficeScan XG contains a vulnerability which could allow remote attackers to execute arbitrary code on affected installations (RCE). An attempted attack requires user authentication. **CVE ID : CVE-2020-8467**	N/A	A-TRE-OFFI-070420/366
Download of Code Without Integrity Check	18-03-2020	6.5	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication. **CVE ID : CVE-2020-8468**	N/A	A-TRE-OFFI-070420/367
Improper Input Validation	18-03-2020	9.4	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not	N/A	A-TRE-OFFI-070420/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required to exploit this vulnerability. **CVE ID : CVE-2020-8470**		
Improper Input Validation	18-03-2020	10	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit this vulnerability. **CVE ID : CVE-2020-8598**	N/A	A-TRE-OFFI-070420/369
Unrestricted Upload of File with Dangerous Type	18-03-2020	10	Trend Micro Apex One (2019) and OfficeScan XG server contain a vulnerable EXE file that could allow a remote attacker to write arbitrary data to an arbitrary path on affected installations and bypass ROOT login. Authentication is not required to exploit this vulnerability. **CVE ID : CVE-2020-8599**	N/A	A-TRE-OFFI-070420/370
worry-free_business_security					
Download of Code Without Integrity Check	18-03-2020	6.5	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could	N/A	A-TRE-WORR-070420/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication. **CVE ID : CVE-2020-8468**		
Improper Input Validation	18-03-2020	9.4	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not required to exploit this vulnerability. **CVE ID : CVE-2020-8470**	N/A	A-TRE-WORR-070420/372
Improper Input Validation	18-03-2020	10	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit this vulnerability. **CVE ID : CVE-2020-8598**	N/A	A-TRE-WORR-070420/373
Improper Limitation of a Pathname to a	18-03-2020	7.5	Trend Micro Worry-Free Business Security (9.0, 9.5, 10.0) is affected by a directory traversal	N/A	A-TRE-WORR-070420/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			vulnerability that could allow an attacker to manipulate a key file to bypass authentication. **CVE ID : CVE-2020-8600**		
typelevel					
http4s					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-03-2020	5	http4s before versions 0.18.26, 0.20.20, and 0.21.2 has a local file inclusion vulnerability. This vulnerability applies to all users of org.http4s.server.staticcontent.FileService, org.http4s.server.staticcontent.ResourceService and org.http4s.server.staticcontent.WebjarService. URI normalization is applied incorrectly. Requests whose path info contain ../ or // can expose resources outside of the configured location. This issue is patched in versions 0.18.26, 0.20.20, and 0.21.2. Note that 0.19.0 is a deprecated release and has never been supported. **CVE ID : CVE-2020-5280**	https://github.com/http4s/http4s/security/advisories/GHSA-66q9-f7ff-mmx6	A-TYP-HTTP-070420/375
Umbraco					
umbraco_cms					
Unrestricted Upload of File with Dangerous Type	16-03-2020	6.5	Umbraco Cloud 8.5.3 allows an authenticated file upload (and consequently Remote Code Execution) via the Install Packages	N/A	A-UMB-UMBR-070420/376

CVSS 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
			functionality. **CVE ID : CVE-2020-9471**		
Unrestricted Upload of File with Dangerous Type	16-03-2020	4	Umbraco CMS 8.5.3 allows an authenticated file upload (and consequently Remote Code Execution) via the Install Package functionality. **CVE ID : CVE-2020-9472**	N/A	A-UMB-UMBR-070420/377
unraid					
unraid					
Improper Control of Generation of Code ('Code Injection')	16-03-2020	10	Unraid through 6.8.0 allows Remote Code Execution. **CVE ID : CVE-2020-5847**	N/A	A-UNR-UNRA-070420/378
Improper Authenticati on	16-03-2020	5	Unraid 6.8.0 allows authentication bypass. **CVE ID : CVE-2020-5849**	N/A	A-UNR-UNRA-070420/379
uppy					
uppy					
Server-Side Request Forgery (SSRF)	20-03-2020	7.5	The uppy npm package < 1.9.3 is vulnerable to a Server-Side Request Forgery (SSRF) vulnerability, which allows an attacker to scan local or external network or otherwise interact with internal systems. **CVE ID : CVE-2020-8135**	N/A	A-UPP-UPPY-070420/380
Vestacp					
vesta_control_panel					
Improper Neutralizatio	22-03-2020	9	Vesta Control Panel (VestaCP) through 0.9.8-	N/A	A-VES-VEST-070420/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			26 allows Command Injection via the schedule/backup Backup Listing Endpoint. The attacker must be able to create a crafted filename on the server, as demonstrated by an FTP session that renames .bash_logout to a .bash_logout' substring followed by shell metacharacters. **CVE ID : CVE-2020-10808**		
videolabs					
libmicrodns					
Uncontrolled Recursion	24-03-2020	5	An exploitable denial-of-service vulnerability exists in the resource record-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing compressed labels in mDNS messages, the compression pointer is followed without checking for recursion, leading to a denial of service. An attacker can send an mDNS message to trigger this vulnerability. **CVE ID : CVE-2020-6071**	N/A	A-VID-LIBM-070420/382
Double Free	24-03-2020	7.5	An exploitable code execution vulnerability exists in the label-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing compressed labels	N/A	A-VID-LIBM-070420/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in mDNS messages, the rr_decode function's return value is not checked, leading to a double free that could be exploited to execute arbitrary code. An attacker can send an mDNS message to trigger this vulnerability. **CVE ID : CVE-2020-6072**		
Integer Overflow or Wraparound	24-03-2020	5	An exploitable denial-of-service vulnerability exists in the TXT record-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing the RDATA section in a TXT record in mDNS messages, multiple integer overflows can be triggered, leading to a denial of service. An attacker can send an mDNS message to trigger this vulnerability. **CVE ID : CVE-2020-6073**	N/A	A-VID-LIBM-070420/384
Out-of-bounds Read	24-03-2020	5	An exploitable denial-of-service vulnerability exists in the message-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing mDNS messages, the implementation does not properly keep track of the available data in the message, possibly leading to an out-of-bounds read that would result in a denial of service. An attacker can send an	N/A	A-VID-LIBM-070420/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mDNS message to trigger this vulnerability. **CVE ID : CVE-2020-6077**		
Unchecked Return Value	24-03-2020	5	An exploitable denial-of-service vulnerability exists in the message-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing mDNS messages in mdns_recv, the return value of the mdns_read_header function is not checked, leading to an uninitialized variable usage that eventually results in a null pointer dereference, leading to service crash. An attacker can send a series of mDNS messages to trigger this vulnerability. **CVE ID : CVE-2020-6078**	N/A	A-VID-LIBM-070420/386
Uncontrolled Resource Consumption	24-03-2020	5	An exploitable denial-of-service vulnerability exists in the resource allocation handling of Videolabs libmicrodns 0.1.0. When encountering errors while parsing mDNS messages, some allocated data is not freed, possibly leading to a denial-of-service condition via resource exhaustion. An attacker can send one mDNS message repeatedly to trigger this vulnerability through decoding of the domain name performed by	N/A	A-VID-LIBM-070420/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rr_decode. **CVE ID : CVE-2020-6079**		
Uncontrolled Resource Consumption	24-03-2020	5	An exploitable denial-of-service vulnerability exists in the resource allocation handling of Videolabs libmicrodns 0.1.0. When encountering errors while parsing mDNS messages, some allocated data is not freed, possibly leading to a denial-of-service condition via resource exhaustion. An attacker can send one mDNS message repeatedly to trigger this vulnerability through the function rr_read_RR [5] reads the current resource record, except for the RDATA section. This is read by the loop at in rr_read. For each RR type, a different function is called. When the RR type is 0x10, the function rr_read_TXT is called at [6]. **CVE ID : CVE-2020-6080**	N/A	A-VID-LIBM-070420/388
Vmware					
remote_console					
Improper Privilege Management	17-03-2020	7.2	VMware Fusion (11.x before 11.5.2), VMware Remote Console for Mac (11.x and prior before 11.0.1) and Horizon Client for Mac (5.x and prior before 5.4.0) contain a privilege escalation	N/A	A-VMW-REMO-070420/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability due to improper use of setuid binaries. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC or Horizon Client is installed. **CVE ID : CVE-2020-3950**		
workstation					
Use After Free	16-03-2020	7.2	VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine. **CVE ID : CVE-2020-3947**	https://www.vmware.com/security/advisories/VMSA-2020-0004.html	A-VMW-WORK-070420/390
Improper Privilege Management	16-03-2020	4.6	Linux Guest VMs running on VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a local privilege escalation vulnerability due to improper file permissions in Cortado Thinprint. Local attackers with non-administrative access to a Linux guest VM with virtual printing	https://www.vmware.com/security/advisories/VMSA-2020-0004.html	A-VMW-WORK-070420/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enabled may exploit this issue to elevate their privileges to root on the same guest VM. **CVE ID : CVE-2020-3948**		
Out-of-bounds Write	17-03-2020	2.1	VMware Workstation (15.x before 15.5.2) and Horizon Client for Windows (5.x and prior before 5.4.0) contain a denial-of-service vulnerability due to a heap-overflow issue in Cortado Thinprint. Attackers with non-administrative access to a guest VM with virtual printing enabled may exploit this issue to create a denial-of-service condition of the Thinprint service running on the system where Workstation or Horizon Client is installed. **CVE ID : CVE-2020-3951**	N/A	A-VMW-WORK-070420/392
fusion					
Use After Free	16-03-2020	7.2	VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition of the vmnetdhcp service	https://www.vmware.com/security/advisories/VMSA-2020-0004.html	A-VMW-FUSI-070420/393

CVSS 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
			running on the host machine. **CVE ID : CVE-2020-3947**		
Improper Privilege Management	16-03-2020	4.6	Linux Guest VMs running on VMware Workstation (15.x before 15.5.2) and Fusion (11.x before 11.5.2) contain a local privilege escalation vulnerability due to improper file permissions in Cortado Thinprint. Local attackers with non-administrative access to a Linux guest VM with virtual printing enabled may exploit this issue to elevate their privileges to root on the same guest VM. **CVE ID : CVE-2020-3948**	https://www.vmware.com/security/advisories/VMSA-2020-0004.html	A-VMW-FUSI-070420/394
Improper Privilege Management	17-03-2020	7.2	VMware Fusion (11.x before 11.5.2), VMware Remote Console for Mac (11.x and prior before 11.0.1) and Horizon Client for Mac (5.x and prior before 5.4.0) contain a privilege escalation vulnerability due to improper use of setuid binaries. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC or Horizon Client is installed. **CVE ID : CVE-2020-3950**	N/A	A-VMW-FUSI-070420/395

CVSS 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
horizon_client					
Improper Privilege Management	17-03-2020	7.2	VMware Fusion (11.x before 11.5.2), VMware Remote Console for Mac (11.x and prior before 11.0.1) and Horizon Client for Mac (5.x and prior before 5.4.0) contain a privilege escalation vulnerability due to improper use of setuid binaries. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC or Horizon Client is installed. **CVE ID : CVE-2020-3950**	N/A	A-VMW-HORI-070420/396
Out-of-bounds Write	17-03-2020	2.1	VMware Workstation (15.x before 15.5.2) and Horizon Client for Windows (5.x and prior before 5.4.0) contain a denial-of-service vulnerability due to a heap-overflow issue in Cortado Thinprint. Attackers with non-administrative access to a guest VM with virtual printing enabled may exploit this issue to create a denial-of-service condition of the Thinprint service running on the system where Workstation or Horizon Client is installed.	N/A	A-VMW-HORI-070420/397

CVSS 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
			CVE ID : CVE-2020-3951		
Weechat					
weechat					
NULL Pointer Dereference	23-03-2020	5	An issue was discovered in WeeChat before 2.7.1 (0.4.0 to 2.7 are affected). A malformed message 352 (who) can cause a NULL pointer dereference in the callback function, resulting in a crash. **CVE ID : CVE-2020-9759**	N/A	A-WEE-WEEC-070420/398
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-03-2020	7.5	An issue was discovered in WeeChat before 2.7.1 (0.3.4 to 2.7 are affected). When a new IRC message 005 is received with longer nick prefixes, a buffer overflow and possibly a crash can happen when a new mode is set for a nick. **CVE ID : CVE-2020-9760**	N/A	A-WEE-WEEC-070420/399
wl-enq_project					
wl-enq					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-03-2020	4.3	Cross-site scripting vulnerability in WL-Enq 1.11 and 1.12 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2020-5559**	N/A	A-WL--WL-E-070420/400
Improper Neutralization of Special Elements used in an OS	25-03-2020	10	WL-Enq 1.11 and 1.12 allows remote attackers to execute arbitrary OS commands with the administrative privilege	N/A	A-WL--WL-E-070420/401

CVSS 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
Command ('OS Command Injection')			via unspecified vectors. **CVE ID : CVE-2020-5560**		
wpforms					
contact_form					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-03-2020	3.5	A stored cross-site scripting (XSS) vulnerability exists in the WPForms Contact Form (aka wpforms-lite) plugin before 1.5.9 for WordPress. **CVE ID : CVE-2020-10385**	N/A	A-WPF-CONT-070420/402
yaml					
pyyaml					
Improper Input Validation	24-03-2020	10	A vulnerability was discovered in the PyYAML library in versions before 5.3.1, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw. An attacker could use this flaw to execute arbitrary code on the system by abusing the python/object/new constructor. **CVE ID : CVE-2020-1747**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1747	A-YAM-PYYA-070420/403

CVSS 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
yargs					
yargs-parser					
Improper Input Validation	16-03-2020	6.4	yargs-parser could be tricked into adding or modifying properties of Object.prototype using a "__proto__" payload. **CVE ID : CVE-2020-7608**	N/A	A-YAR-YARG-070420/404
Zend					
Zendto					
Origin Validation Error	24-03-2020	5	lib/NSSDropbox.php in ZendTo prior to 5.22-2 Beta allowed IP address spoofing via the X-Forwarded-For header. **CVE ID : CVE-2020-8984**	N/A	A-ZEN-ZEND-070420/405
Cross-Site Request Forgery (CSRF)	24-03-2020	6.8	ZendTo prior to 5.22-2 Beta allowed reflected XSS and CSRF via the unlock.tpl unlock user functionality. **CVE ID : CVE-2020-8985**	N/A	A-ZEN-ZEND-070420/406
Improper Check for Unusual or Exceptional Conditions	24-03-2020	7.5	lib/NSSDropbox.php in ZendTo prior to 5.22-2 Beta failed to properly check for equality when validating the session cookie, allowing an attacker to gain administrative access with a large number of requests. **CVE ID : CVE-2020-8986**	N/A	A-ZEN-ZEND-070420/407
Zimbra					
zm-mailbox					
Incorrect Authorizatio	20-03-2020	4	cs/service/account/AutoCompleteGal.java in Zimbra	https://github.com/Zim	A-ZIM-ZM-M-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			zm-mailbox before 8.8.15.p8 allows authenticated users to request any GAL account. This differs from the intended behavior in which the domain of the authenticated user must match the domain of the galsync account in the request. **CVE ID : CVE-2020-10194**	bra/zm-mailbox/pull/1020	070420/408
zim-wiki					
zim					
Improper Input Validation	23-03-2020	2.1	Zim through 0.72.1 creates temporary directories with predictable names. A malicious user could predict and create Zim's temporary directories and prevent other users from being able to start Zim, resulting in a denial of service. **CVE ID : CVE-2020-10870**	N/A	A-ZIM-ZIM-070420/409
Zohocorp					
manageengine_desktop_central					
Information Exposure	30-03-2020	5	Zoho ManageEngine Desktop Central allows unauthenticated users to access PDFGenerationServlet, leading to sensitive information disclosure. **CVE ID : CVE-2020-8509**	https://www.manageengine.com/products/desktop-central/unauthenticated-servlet-access.html	A-ZOH-MANA-070420/410

CVSS 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
manageengine_password_manager_pro					
Cross-Site Request Forgery (CSRF)	16-03-2020	6.8	Zoho ManageEngine Password Manager Pro 10.4 and prior has no protection against Cross-site Request Forgery (CSRF) attacks, as demonstrated by changing a user's role. **CVE ID : CVE-2020-9346**	N/A	A-ZOH-MANA-070420/411
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-03-2020	7.5	** DISPUTED ** Zoho ManageEngine Password Manager Pro through 10.x has a CSV Excel Macro Injection vulnerability via a crafted name that is mishandled by the Export Passwords feature. NOTE: the vendor disputes the significance of this report because they expect CSV risk mitigation to be provided by an external application, and do not plan to add CSV constraints to their own products. **CVE ID : CVE-2020-9347**	N/A	A-ZOH-MANA-070420/412
manageengine_assetexplorer					
Improper Validation of Integrity Check Value	23-03-2020	4.9	An issue was discovered in Zoho ManageEngine AssetExplorer 6.5. During an upgrade of the Windows agent, it does not validate the source and binary downloaded. This allows an attacker on an adjacent network to execute code with NT	https://www.manageengine.com/products/asset-explorer/sp-readme.html	A-ZOH-MANA-070420/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AUTHORITY/SYSTEM privileges on the agent machines by providing an arbitrary executable via a man-in-the-middle attack. **CVE ID : CVE-2020-8838**		
zulipchat					
zulip_desktop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-03-2020	4.3	Zulip Desktop before 4.0.3 loaded untrusted content in an Electron webview with web security disabled, which can be exploited for XSS in a number of ways. This especially affects Zulip Desktop 2.3.82. **CVE ID : CVE-2020-9443**	https://blog.zulip.org/2020/02/29/zulip-desktop-4-0-3-security-release/	A-ZUL-ZULI-070420/414
Operating System					
Apple					
mac_os					
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3770**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/415
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to information disclosure. **CVE ID : CVE-2020-3771**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3772**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/417
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3773**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/418
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3774**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/419
Improper Restriction of Operations within the Bounds of a	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability.	https://helpx.adobe.com/security/products/photoshop/apsb	O-APP-MAC_-070420/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3775**	20-14.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3776**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/421
Out-of-bounds Read	25-03-2020	5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3777**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/422
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3778**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/423
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/424

CVSS 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
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3779**		
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3780**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/425
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3781**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/426
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3782**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/427
Improper Restriction of Operations within the Bounds of a	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a heap corruption vulnerability.	https://helpx.adobe.com/security/products/photoshop/apsb	O-APP-MAC_-070420/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3783**	20-14.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3784**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/429
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3785**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/430
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3786**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-APP-MAC_-070420/431
Improper Restriction of Operations within the	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory	https://helpx.adobe.com/security/products/photoshop/apsb	O-APP-MAC_-070420/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3787**	20-14.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3788**	https://help x.adobe.com /security/pr oducts/phot oshop/apsb 20-14.html	O-APP-MAC_- 070420/433
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3789**	https://help x.adobe.com /security/pr oducts/phot oshop/apsb 20-14.html	O-APP-MAC_- 070420/434
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3790**	https://help x.adobe.com /security/pr oducts/phot oshop/apsb 20-14.html	O-APP-MAC_- 070420/435
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and	https://help x.adobe.com /security/pr oducts/phot	O-APP-MAC_- 070420/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3791**	oshop/apsb20-14.html	
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3792**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/437
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3793**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/438
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier,	https://helpx.adobe.com/security/pr	O-APP-MAC_-070420/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3795**	oducts/acrobat/apsb20-13.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3797**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/440
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a stack-based buffer overflow vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2020-3799**		
Improper Release of Memory Before Removing Last Reference	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory address leak vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3800**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/442
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3801**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/443
Use After Free	25-03-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3802**		
Untrusted Search Path	25-03-2020	4.4	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-3803**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/445
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3804**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/446

CVSS 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
Use After Free	25-03-2020	10	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3805**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/447
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3806**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/448
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a buffer	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-APP-MAC_-070420/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3807**		
Improper Privilege Management	17-03-2020	7.2	VMware Fusion (11.x before 11.5.2), VMware Remote Console for Mac (11.x and prior before 11.0.1) and Horizon Client for Mac (5.x and prior before 5.4.0) contain a privilege escalation vulnerability due to improper use of setuid binaries. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC or Horizon Client is installed. **CVE ID : CVE-2020-3950**	N/A	O-APP-MAC_-070420/450
Canon					
oce_colorwave_500_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	4.3	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Stored XSS in /TemplateManager/indexExternalLocation.jsp. The vulnerable parameter is map(template_name). NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10667**	N/A	O-CAN-OCE_-070420/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	4.3	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Reflected XSS in /home.jsp. The vulnerable parameter is openSI. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10668**	N/A	O-CAN-OCE_-070420/452
Improper Authentication	19-03-2020	5	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to authentication bypass on the page /home.jsp. An unauthenticated attacker able to connect to the device's web interface can get a copy of the documents uploaded by any users. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10669**	N/A	O-CAN-OCE_-070420/453
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	4.3	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Reflected XSS in the parameter settingId of the settingDialogContent.jsp page. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10670**	N/A	O-CAN-OCE_-070420/454
Cross-Site Request	19-03-2020	6.8	The Canon Oce Colorwave 500 4.0.0.0 printer's web	N/A	O-CAN-OCE_-070420/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			application is missing any form of CSRF protections. This is a system-wide issue. An attacker could perform administrative actions by targeting a logged-in administrative user. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10671**		
Cisco					
sd-wan_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**	N/A	O-CIS-SD-W-070420/456
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate	N/A	O-CIS-SD-W-070420/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**	N/A	O-CIS-SD-W-070420/458
Debian					
debian_linux					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	18-03-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.aries.transaction.jms.internal.XaPooledConnectionFactory (aka aries.transaction.jms). **CVE ID : CVE-2020-10672**	N/A	O-DEB-DEBI-070420/459
N/A	18-03-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.caucho.config.types.ResourceRef (aka caucho-quercus). **CVE ID : CVE-2020-10673**	N/A	O-DEB-DEBI-070420/460
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-03-2020	6	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability has been discovered where certain parameters are not properly escaped when generating certain queries for search actions in libraries/classes/Controllers/Table/TableSearchController.php. An attacker can generate a crafted database or table name. The attack can be performed if a user attempts certain search	N/A	O-DEB-DEBI-070420/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations on the malicious database or table. **CVE ID : CVE-2020-10802**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-03-2020	3.5	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was discovered where malicious code could be used to trigger an XSS attack through retrieving and displaying results (in tbl_get_field.php and libraries/classes/Display/Results.php). The attacker must be able to insert crafted data into certain database tables, which when retrieved (for instance, through the Browse tab) can trigger the XSS attack. **CVE ID : CVE-2020-10803**	N/A	O-DEB-DEBI-070420/462
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	3.5	In ActionView before versions 6.0.2.2 and 5.2.4.2, there is a possible XSS vulnerability in ActionView's JavaScript literal escape helpers. Views that use the `j` or `escape_javascript` methods may be susceptible to XSS attacks. The issue is fixed in versions 6.0.2.2 and 5.2.4.2.	https://github.com/rails/rails/security/advisories/GHSA-65cv-r6x7-79hv	O-DEB-DEBI-070420/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5267		
Improper Input Validation	23-03-2020	6.8	Insufficient policy enforcement in media in Google Chrome prior to 80.0.3987.132 allowed a remote attacker to bypass same origin policy via a crafted HTML page. **CVE ID : CVE-2020-6420**	N/A	O-DEB-DEBI-070420/464
Use After Free	23-03-2020	9.3	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6422**	N/A	O-DEB-DEBI-070420/465
Use After Free	23-03-2020	9.3	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6424**	N/A	O-DEB-DEBI-070420/466
Improper Input Validation	23-03-2020	5.8	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.149 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension. **CVE ID : CVE-2020-6425**	N/A	O-DEB-DEBI-070420/467
Improper Restriction of	23-03-2020	4.3	Inappropriate implementation in V8 in Google Chrome prior to	N/A	O-DEB-DEBI-070420/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6426**		
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6427**	N/A	O-DEB-DEBI-070420/469
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6428**	N/A	O-DEB-DEBI-070420/470
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6429**	N/A	O-DEB-DEBI-070420/471
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6449**	N/A	O-DEB-DEBI-070420/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	24-03-2020	6.8	KDE Okular before 1.10.0 allows code execution via an action link in a PDF document. **CVE ID : CVE-2020-9359**	https://invent.kde.org/kde/okular/-/commit/6a93a033b4f9248b3cd4d04689b8391df754e244, https://kde.org/info/security/advisory-20200312-1.txt	O-DEB-DEBI-070420/473
Dlink					
dir-882_firmware					
Improper Authentication	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper implementation of the authentication algorithm. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-9470. **CVE ID : CVE-2020-8863**	N/A	O-DLI-DIR--070420/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Comparison	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of empty passwords. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9471. **CVE ID : CVE-2020-8864**	N/A	O-DLI-DIR--070420/475
dir-867_firmware					
Improper Authenticati on	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper implementation of the	N/A	O-DLI-DIR--070420/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication algorithm. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-9470. **CVE ID : CVE-2020-8863**		
Incorrect Comparison	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of empty passwords. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9471. **CVE ID : CVE-2020-8864**	N/A	O-DLI-DIR--070420/477
dir-878_firmware					
Improper Authentication	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04.	N/A	O-DLI-DIR--070420/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper implementation of the authentication algorithm. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-9470. **CVE ID : CVE-2020-8863**		
Incorrect Comparison	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of empty passwords. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9471. **CVE ID : CVE-2020-8864**	N/A	O-DLI-DIR--070420/479
Draytek					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vigor2960_firmware					
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi through ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 2 of 3). **CVE ID : CVE-2020-10824**	N/A	O-DRA-VIGO-070420/480
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi while base64 decoding ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 3 of 3). **CVE ID : CVE-2020-10825**	N/A	O-DRA-VIGO-070420/481
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-03-2020	10	/cgi-bin/activate.cgi on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve command injection via a remote HTTP request in DEBUG mode. **CVE ID : CVE-2020-10826**	N/A	O-DRA-VIGO-070420/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in apmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10827**	N/A	O-DRA-VIGO-070420/483
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in cvmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10828**	N/A	O-DRA-VIGO-070420/484
vigor300b_firmware					
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi through ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 2 of 3). **CVE ID : CVE-2020-10824**	N/A	O-DRA-VIGO-070420/485
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi while base64 decoding ticket parameter on Draytek	N/A	O-DRA-VIGO-070420/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 3 of 3). **CVE ID : CVE-2020-10825**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-03-2020	10	/cgi-bin/activate.cgi on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve command injection via a remote HTTP request in DEBUG mode. **CVE ID : CVE-2020-10826**	N/A	O-DRA-VIGO-070420/487
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in apmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10827**	N/A	O-DRA-VIGO-070420/488
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in cvmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-**	N/A	O-DRA-VIGO-070420/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10828		
vigor3900_firmware					
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi through ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 2 of 3). **CVE ID : CVE-2020-10824**	N/A	O-DRA-VIGO-070420/490
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi while base64 decoding ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 3 of 3). **CVE ID : CVE-2020-10825**	N/A	O-DRA-VIGO-070420/491
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-03-2020	10	/cgi-bin/activate.cgi on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve command injection via a remote HTTP request in DEBUG mode. **CVE ID : CVE-2020-**	N/A	O-DRA-VIGO-070420/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10826		
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in apmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10827**	N/A	O-DRA-VIGO-070420/493
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in cvmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10828**	N/A	O-DRA-VIGO-070420/494
Fedoraproject					
fedora					
Improper Input Validation	24-03-2020	10	A vulnerability was discovered in the PyYAML library in versions before 5.3.1, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw. An attacker could use this flaw to execute arbitrary	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1747	O-FED-FEDO-070420/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code on the system by abusing the python/object/new constructor. **CVE ID : CVE-2020-1747**		
Use After Free	23-03-2020	9.3	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6422**	N/A	O-FED-FEDO-070420/496
Use After Free	23-03-2020	9.3	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6424**	N/A	O-FED-FEDO-070420/497
Improper Input Validation	23-03-2020	5.8	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.149 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension. **CVE ID : CVE-2020-6425**	N/A	O-FED-FEDO-070420/498
Improper Restriction of Operations within the Bounds of a Memory	23-03-2020	4.3	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted	N/A	O-FED-FEDO-070420/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			HTML page. **CVE ID : CVE-2020-6426**		
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6427**	N/A	O-FED-FEDO-070420/500
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6428**	N/A	O-FED-FEDO-070420/501
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6429**	N/A	O-FED-FEDO-070420/502
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6449**	N/A	O-FED-FEDO-070420/503
Improper Input Validation	24-03-2020	6.8	KDE Okular before 1.10.0 allows code execution via an action link in a PDF document.	https://invent.kde.org/kde/okular/-/commit/6a	O-FED-FEDO-070420/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9359	93a033b4f9248b3cd4d04689b8391df754e244, https://kde.org/info/security/advisory-20200312-1.txt	
Google					
android					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) (Exynos chipsets) software. Kernel Wi-Fi drivers allow out-of-bounds Read or Write operations (e.g., a buffer overflow). The Samsung IDs are SVE-2019-16125, SVE-2019-16134, SVE-2019-16158, SVE-2019-16159, SVE-2019-16319, SVE-2019-16320, SVE-2019-16337, SVE-2019-16464, SVE-2019-16465, SVE-2019-16467 (March 2020). **CVE ID : CVE-2020-10832**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/505
Improper Authentication	24-03-2020	5	An issue was discovered on Samsung mobile devices with Q(10.0) software. The DeX Lockscreen allows attackers to access the quick panel and notifications. The Samsung	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID is SVE-2019-16532 (March 2020). **CVE ID : CVE-2020-10833**		
Information Exposure	24-03-2020	5	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can view notifications on the lock screen via Routines. The Samsung ID is SVE-2019-15074 (February 2020). **CVE ID : CVE-2020-10834**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/507
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-03-2020	7.5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos chipsets) software. The Widevine Trustlet allows read and write operations on arbitrary memory locations. The Samsung ID is SVE-2019-15873 (February 2020). **CVE ID : CVE-2020-10836**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/508
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-03-2020	10	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (with TEEGRIS) software. The Esecomm Trustlet allows a stack overflow and arbitrary code execution. The Samsung ID is SVE-2019-15984 (February 2020). **CVE ID : CVE-2020-**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10837		
Use After Free	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. PROCA allows a use-after-free and arbitrary code execution. The Samsung ID is SVE-2019-16132 (February 2020). **CVE ID : CVE-2020-10838**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/510
Incorrect Authorization	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can bypass Factory Reset Protection (FRP) via a SIM card. The Samsung ID is SVE-2019-16193 (February 2020). **CVE ID : CVE-2020-10839**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/511
Improper Release of Memory Before Removing Last Reference	24-03-2020	3.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 9610 chipsets) software. There is a kernel pointer leak in the vipx driver. The Samsung ID is SVE-2019-16293 (February 2020). **CVE ID : CVE-2020-10840**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/512
N/A	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 9610 chipsets) software. There	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/513

CVSS 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
			is an arbitrary kfree in the vipx and vertex drivers. The Samsung ID is SVE-2019-16294 (February 2020). **CVE ID : CVE-2020-10841**		
Out-of-bounds Write	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (S.LSI chipsets) software. There is a heap out-of-bounds write in the tsmux driver. The Samsung ID is SVE-2019-16295 (February 2020). **CVE ID : CVE-2020-10842**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/514
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	24-03-2020	4.4	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (S.LSI chipsets) software. There are race conditions in the hdcp2 driver. The Samsung ID is SVE-2019-16296 (February 2020). **CVE ID : CVE-2020-10843**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/515
Out-of-bounds Read	24-03-2020	6.4	An issue was discovered on Samsung mobile devices with O(8.x), P(9.x), and Q(10.0) software. There is an out-of-bounds read vulnerability in media.audio_policy. The Samsung ID is SVE-2019-16333 (February 2020).	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10844		
Use After Free	24-03-2020	4.4	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. There is a race condition leading to a use-after-free in MTP. The Samsung ID is SVE-2019-16520 (February 2020). **CVE ID : CVE-2020-10845**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/517
Improper Input Validation	24-03-2020	1.9	An issue was discovered on Samsung mobile devices with P(9.x) and Q(10.x) software. Attackers can enable the OEM unlock feature on a KG-enrolled devices, leading to potentially unwanted binaries being downloaded. The Samsung ID is SVE-2019-16554 (February 2020). **CVE ID : CVE-2020-10846**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/518
Improper Authentication	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) (Galaxy S8 and Note8) software. Facial recognition can be spoofed. The Samsung ID is SVE-2019-16614 (February 2020). **CVE ID : CVE-2020-10847**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/519
Out-of-	24-03-2020	4.6	An issue was discovered	https://secu	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			on Samsung mobile devices with O(8.0), P(9.0), and Q(10.0) (Broadcom chipsets) software. A kernel driver heap overflow leads to arbitrary code execution. The Samsung ID is SVE-2019-15880 (March 2020). **CVE ID : CVE-2020-10829**	rity.samsung mobile.com/ securityUpd ate.smsb	070420/520
Information Exposure	24-03-2020	2.1	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can view notifications by entering many PINs in Lockdown mode. The Samsung ID is SVE-2019-16590 (March 2020). **CVE ID : CVE-2020-10830**	https://secu rity.samsung mobile.com/ securityUpd ate.smsb	O-GOO-ANDR-070420/521
Insufficient Verification of Data Authenticity	24-03-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can trigger an update to arbitrary touch-screen firmware. The Samsung ID is SVE-2019-16013 (March 2020). **CVE ID : CVE-2020-10831**	https://secu rity.samsung mobile.com/ securityUpd ate.smsb	O-GOO-ANDR-070420/522
Improper Restriction of Operations	24-03-2020	10	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos 9810	https://secu rity.samsung mobile.com/ securityUpd	O-GOO-ANDR-070420/523

CVSS 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
within the Bounds of a Memory Buffer			chipsets) software. Arbitrary memory mapping exists in TEE. The Samsung ID is SVE-2019-16665 (February 2020). **CVE ID : CVE-2020-10848**	ate.smsb	
Improper Restriction of Excessive Authentication Attempts	24-03-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos7885, Exynos8895, and Exynos9810 chipsets) software. The Gatekeeper trustlet allows a brute-force attack on the screen lock password. The Samsung ID is SVE-2019-14575 (January 2020). **CVE ID : CVE-2020-10849**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/524
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-03-2020	10	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos chipsets) software. The secure bootloade has a buffer overflow of the USB buffer, leading to arbitrary code execution. The Samsung ID is SVE-2019-15872 (January 2020). **CVE ID : CVE-2020-10850**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/525
Out-of-bounds Write	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. There is	https://security.samsungmobile.com/securityUpd	O-GOO-ANDR-070420/526

CVSS 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
			a stack overflow in the kperfmon driver. The Samsung ID is SVE-2019-15876 (January 2020). **CVE ID : CVE-2020-10851**	ate.smsb	
Out-of-bounds Write	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. There is a stack overflow in display driver. The Samsung ID is SVE-2019-15877 (January 2020). **CVE ID : CVE-2020-10852**	N/A	O-GOO-ANDR-070420/527
Information Exposure	24-03-2020	5	An issue was discovered on Samsung mobile devices with P(9.0) software. Gallery leaks cached data. The Samsung IDs are SVE-2019-16010, SVE-2019-16011, SVE-2019-16012 (January 2020). **CVE ID : CVE-2020-10853**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/528
Information Exposure	24-03-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Kernel stack addresses are leaked to userspace. The Samsung ID is SVE-2019-16161 (January 2020). **CVE ID : CVE-2020-10854**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-070420/529
Improper Input	24-03-2020	2.1	An issue was discovered on Samsung mobile	https://security.samsung	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			devices with P(9.0) software. Attackers can bypass Factory Reset Protection (FRP) via AppTray. The Samsung ID is SVE-2019-16192 (January 2020). **CVE ID : CVE-2020-10855**	mobile.com/securityUpdate.smsb	070420/530
Grandstream					
ucm6204_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5724**	https://www.tenable.com/security/research/tra-2020-17	O-GRA-UCM6-070420/531
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	4.3	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords. **CVE ID : CVE-2020-5725**	https://www.tenable.com/security/research/tra-2020-17	O-GRA-UCM6-070420/532
Improper Neutralization of Special	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to	https://www.tenable.com/security/	O-GRA-UCM6-070420/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5726**	research/tra-2020-17	
ucm6200_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-03-2020	10	The HTTP interface of the Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via crafted HTTP request. An attacker can use this vulnerability to execute shell commands as root on versions before 1.0.19.20 or inject HTML in password recovery emails in versions before 1.0.20.17. **CVE ID : CVE-2020-5722**	N/A	O-GRA-UCM6-070420/534
ucm6202_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5724**	https://www.tenable.com/security/research/tra-2020-17	O-GRA-UCM6-070420/535
Improper Neutralization of Special	30-03-2020	4.3	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to	https://www.tenable.com/security/	O-GRA-UCM6-070420/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords. **CVE ID : CVE-2020-5725**	research/tra-2020-17	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5726**	https://www.tenable.com/security/research/tra-2020-17	O-GRA-UCM6-070420/537
ucm6208_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5724**	https://www.tenable.com/security/research/tra-2020-17	O-GRA-UCM6-070420/538
Improper Neutralization of Special Elements used in an	30-03-2020	4.3	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify	https://www.tenable.com/security/research/tra-2020-17	O-GRA-UCM6-070420/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords. **CVE ID : CVE-2020-5725**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5726**	https://www.tenable.com/security/research/tra-2020-17	O-GRA-UCM6-070420/540
Huawei					
mate_30_pro_firmware					
Improper Authentication	20-03-2020	2.1	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier	N/A	O-HUA-MATE-070420/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1793**		
Improper Authentication	20-03-2020	2.1	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1794**	N/A	O-HUA-MATE-070420/542
N/A	20-03-2020	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations.Affected product versions include:HUAWEI Mate 20	N/A	O-HUA-MATE-070420/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1795**		
Incorrect Authorization	20-03-2020	4.6	There is an improper authorization vulnerability in several smartphones. The software incorrectly performs an authorization to certain user, successful exploit could allow a low privilege user to do certain operation which the user are supposed not to do.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1796**	N/A	O-HUA-MATE-070420/544
oxfords-an00a_firmware					
Improper Authentication	20-03-2020	2.1	Huawei smartphone OxfordS-AN00A with versions earlier than 10.0.1.152D(C735E152R3P3),versions earlier than 10.0.1.160(C00E160R4P1) have an improper authentication	N/A	O-HUA-OXFO-070420/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Authentication to target component is improper when device performs an operation. Attackers exploit this vulnerability to obtain some information by loading malicious application, leading to information leak. **CVE ID : CVE-2020-1878**		
oxfordp-an10b_firmware					
Improper Authentication	26-03-2020	6.8	Huawei smartphones OxfordP-AN10B with versions earlier than 10.0.1.169(C00E166R4P1) have an improper authentication vulnerability. The Application doesn't perform proper authentication when user performs certain operations. An attacker can trick user into installing a malicious plug-in to exploit this vulnerability. Successful exploit could allow the attacker to bypass the authentication to perform unauthorized operations. **CVE ID : CVE-2020-9066**	N/A	O-HUA-OXFO-070420/546
taurus-al00b_firmware					
Use After Free	26-03-2020	2.1	Huawei smart phone Taurus-AL00B with versions earlier than 10.0.0.203(C00E201R7P2)	N/A	O-HUA-TAUR-070420/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have a use-after-free (UAF) vulnerability. An authenticated, local attacker may perform specific operations to exploit this vulnerability. Successful exploitation may tamper with the information to affect the availability. **CVE ID : CVE-2020-9065**		
secospace_antiddos8000_firmware					
Improper Authenticati on	20-03-2020	6.8	Some Huawei products have a security vulnerability due to improper authentication. A remote attacker needs to obtain some information and forge the peer device to send specific packets to the affected device. Due to the improper implementation of the authentication function, attackers can exploit the vulnerability to connect to affected devices and execute a series of commands.Affected product versions include:Secospace AntiDDoS8000 versions V500R001C00,V500R001C20,V500R001C60,V500R005C00. **CVE ID : CVE-2020-1864**	N/A	O-HUA-SECO-070420/548
p30_firmware					
Incorrect Authorizatio	26-03-2020	6.8	HUAWEI smartphones P30 with versions earlier	N/A	O-HUA-P30_-070420/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			than 10.0.0.185(C00E85R1P11) have an improper access control vulnerability. The software incorrectly restricts access to a function interface from an unauthorized actor, the attacker tricks the user into installing a crafted application, successful exploit could allow the attacker do certain unauthenticated operations. **CVE ID : CVE-2020-1800**		
mate_20_firmware					
Improper Authenticati on	20-03-2020	2.1	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2) . **CVE ID : CVE-2020-1793**	N/A	O-HUA-MATE-070420/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-03-2020	2.1	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1794**	N/A	O-HUA-MATE-070420/551
N/A	20-03-2020	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier	N/A	O-HUA-MATE-070420/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1795**		
Incorrect Authorization	20-03-2020	4.6	There is an improper authorization vulnerability in several smartphones. The software incorrectly performs an authorization to certain user, successful exploit could allow a low privilege user to do certain operation which the user are supposed not to do.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1796**	N/A	O-HUA-MATE-070420/553
osca-550_firmware					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560	N/A	O-HUA-OSCA-070420/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**		
osca-550a_firmware					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**	N/A	O-HUA-OSCA-070420/555
osca-550ax_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**	N/A	O-HUA-OSCA-070420/556
osca-550x_firmware					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions	N/A	O-HUA-OSCA-070420/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**		
hege-560_firmware					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**	N/A	O-HUA-HEGE-070420/558
hege-570_firmware					
Improper	20-03-2020	3.6	There is an improper	N/A	O-HUA-HEGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Integrity Check Value			integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**		070420/559
insulet					
omnipod_insulin_management_system_firmware					
Incorrect Authorization	20-03-2020	4.6	The affected insulin pump is designed to communicate using a wireless RF with an Insulet manufactured Personal Diabetes Manager device. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with access to one of the affected insulin	N/A	O-INS-OMNI-070420/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pump models may be able to modify and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery. **CVE ID : CVE-2020-10597**		
Linux					
linux_kernel					
Out-of-bounds Write	24-03-2020	4.9	In the Linux kernel before 5.5.8, get_raw_socket in drivers/vhost/net.c lacks validation of an sk_family field, which might allow attackers to trigger kernel stack corruption via crafted system calls. **CVE ID : CVE-2020-10942**	N/A	O-LIN-LINU-070420/561
Microsoft					
windows					
Unrestricted Upload of File with Dangerous Type	25-03-2020	7.5	Serendipity before 2.3.4 on Windows allows remote attackers to execute arbitrary code because the filename of a renamed file may end with a dot. This file may then be renamed to have a .php filename. **CVE ID : CVE-2020-10964**	N/A	O-MIC-WIND-070420/562
Out-of-bounds Read	20-03-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected	N/A	O-MIC-WIND-070420/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9624. **CVE ID : CVE-2020-8877**		
Out-of-bounds Write	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated	N/A	O-MIC-WIND-070420/564

CVSS 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
			structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9625. **CVE ID : CVE-2020-8878**		
Out-of-bounds Read	20-03-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9626. **CVE ID : CVE-2020-8879**	N/A	O-MIC-WIND-070420/565
Out-of-bounds Read	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction	N/A	O-MIC-WIND-070420/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9773. **CVE ID : CVE-2020-8880**		
Use After Free	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-	N/A	O-MIC-WIND-070420/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9774. **CVE ID : CVE-2020-8881**		
Access of Uninitialized Pointer	20-03-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the PSD files. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9811. **CVE ID : CVE-2020-8882**	N/A	O-MIC-WIND-070420/568
Out-of-bounds Read	20-03-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack	N/A	O-MIC-WIND-070420/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9880. **CVE ID : CVE-2020-8883**		
Improper Input Validation	20-03-2020	4.3	An issue was discovered in signotec signoPAD-API/Web (formerly Websocket Pad Server) before 3.1.1 on Windows. It is possible to perform a Denial of Service attack because the implementation doesn't limit the parsing of nested JSON structures. If a victim visits an attacker-controlled website, this vulnerability can be exploited via WebSocket data with a deeply nested JSON array. **CVE ID : CVE-2020-9343**	N/A	O-MIC-WIND-070420/570
Allocation of Resources Without Limits or Throttling	20-03-2020	4.3	An issue was discovered in signotec signoPAD-API/Web (formerly Websocket Pad Server) before 3.1.1 on Windows. It is possible to perform a Denial of Service attack because the application doesn't limit the number of opened WebSocket	N/A	O-MIC-WIND-070420/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sockets. If a victim visits an attacker-controlled website, this vulnerability can be exploited. **CVE ID : CVE-2020-9345**		
Improper Certificate Validation	18-03-2020	4	Entrust Entelligence Security Provider (ESP) before 10.0.60 on Windows mishandles errors during SSL Certificate Validation, leading to situations where (for example) a user continues to interact with a web site that has an invalid certificate chain. **CVE ID : CVE-2020-10659**	N/A	O-MIC-WIND-070420/572
Incorrect Default Permissions	25-03-2020	7.5	Adobe Genuine Integrity Service versions Version 6.4 and earlier have an insecure file permissions vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-3766**	https://helpx.adobe.com/security/products/integrity_service/apsb20-12.html	O-MIC-WIND-070420/573
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3770**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/574
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop	https://helpx.adobe.com/security/pr	O-MIC-WIND-070420/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3771**	oducts/photoshop/apsb20-14.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3772**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/576
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3773**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/577
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3774**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/578
Improper Restriction	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and	https://helpx.adobe.com	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3775**	/security/products/photoshop/apsb20-14.html	070420/579
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3776**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/580
Out-of-bounds Read	25-03-2020	5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3777**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/581
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3778**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/582
Out-of-bounds	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop	https://helpx.adobe.com/security/pr	O-MIC-WIND-070420/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3779**	oducts/photoshop/apsb20-14.html	
Out-of-bounds Write	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3780**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/584
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3781**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/585
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3782**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/586
Improper Restriction	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and	https://helpx.adobe.com	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			earlier, and Photoshop 2020 versions 21.1 and earlier have a heap corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3783**	/security/products/photoshop/apsb20-14.html	070420/587
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3784**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/588
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3785**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/589
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3786**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3787**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/591
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3788**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/592
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3789**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/593
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	6.8	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/594

CVSS 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
			CVE ID : CVE-2020-3790		
Out-of-bounds Read	25-03-2020	4.3	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3791**	https://helpx.adobe.com/security/products/photoshop/apsb20-14.html	O-MIC-WIND-070420/595
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3792**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/596
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution . **CVE ID : CVE-2020-3793**		
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3795**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/598
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3797**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/599
Out-of-bounds Write	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 2015.006.30510 and earlier have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3799**		
Improper Release of Memory Before Removing Last Reference	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory address leak vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3800**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/601
Use After Free	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3801**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/602
Use After	25-03-2020	6.8	Adobe Acrobat and Reader	https://help	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3802**	x.adobe.com /security/pr oducts/acro bat/apsb20-13.html	070420/603
Untrusted Search Path	25-03-2020	4.4	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-3803**	https://help x.adobe.com /security/pr oducts/acro bat/apsb20-13.html	O-MIC-WIND-070420/604
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-	https://help x.adobe.com /security/pr oducts/acro bat/apsb20-13.html	O-MIC-WIND-070420/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3804**		
Use After Free	25-03-2020	10	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3805**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/606
Out-of-bounds Read	25-03-2020	5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3806**	https://helpx.adobe.com/security/products/acrobat/apsb20-13.html	O-MIC-WIND-070420/607
Buffer Copy without Checking Size of Input	25-03-2020	7.5	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and	https://helpx.adobe.com/security/products/acro	O-MIC-WIND-070420/608

CVSS 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
('Classic Buffer Overflow')			earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-3807**	bat/apsb20-13.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	25-03-2020	5.8	Creative Cloud Desktop Application versions 5.0 and earlier have a time-of-check to time-of-use (toctou) race condition vulnerability. Successful exploitation could lead to arbitrary file deletion. **CVE ID : CVE-2020-3808**	https://helpx.adobe.com/security/products/creative-cloud/apsb20-11.html	O-MIC-WIND-070420/609
Out-of-bounds Write	17-03-2020	2.1	VMware Workstation (15.x before 15.5.2) and Horizon Client for Windows (5.x and prior before 5.4.0) contain a denial-of-service vulnerability due to a heap-overflow issue in Cortado Thinprint. Attackers with non-administrative access to a guest VM with virtual printing enabled may exploit this issue to create a denial-of-service condition of the Thinprint service running on the system where Workstation or Horizon Client is installed.	N/A	O-MIC-WIND-070420/610

CVSS 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
			CVE ID : CVE-2020-3951		
Out-of-bounds Write	25-03-2020	6.8	Adobe Bridge versions 10.0 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9551**	https://helpx.adobe.com/security/products/bridge/apsb20-17.html	O-MIC-WIND-070420/611
Out-of-bounds Write	25-03-2020	6.8	Adobe Bridge versions 10.0 have a heap-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9552**	https://helpx.adobe.com/security/products/bridge/apsb20-17.html	O-MIC-WIND-070420/612
Mikrotik					
hex_lite_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-HEX_-070420/613
hex_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new	N/A	O-MIK-HEX_-070420/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
hex_poe_lite_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-HEX_-070420/615
powerbox_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-POWE-070420/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hex_s_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-HEX_-070420/617
hex_poe_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-HEX_-070420/618
rb2011il-in_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via	N/A	O-MIK-RB20-070420/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
rb2011il-rm_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-RB20-070420/620
powerbox_pro_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-POWE-070420/621
rb2011ils-in_firmware					
Uncontrolled	23-03-2020	5	The SSH daemon on	N/A	O-MIK-RB20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		070420/622
rb2011uias-in_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-RB20-070420/623
rb2011uias-rm_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of	N/A	O-MIK-RB20-070420/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uncontrolled resource management. **CVE ID : CVE-2020-10364**		
rb3011uias-rm_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-RB30-070420/625
rb4011igs\+rm_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-RB40-070420/626
rb1100ahx4_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow	N/A	O-MIK-RB11-070420/627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
ccr1009-7g-1c-pc_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-CCR1-070420/628
ccr1009-7g-1c-1s\+pc_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management.	N/A	O-MIK-CCR1-070420/629

CVSS 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
			CVE ID : CVE-2020-10364		
ccr1009-7g-1c-1s\+_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-CCR1-070420/630
ccr1016-12g_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-CCR1-070420/631
ccr1016-12s-1s\+_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new	N/A	O-MIK-CCR1-070420/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
ccr1036-12g-4s_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-CCR1-070420/633
ccr1036-8g-2s\+_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-CCR1-070420/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ccr1036-12g-4s-em_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-CCR1-070420/635
ccr1036-8g-2s\+em_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	O-MIK-CCR1-070420/636
ccr1072-1g-8s\+_firmware					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via	N/A	O-MIK-CCR1-070420/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
Mitsubishielectric					
iu1-1m20-d_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-03-2020	7.5	Buffer error vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5542**	N/A	O-MIT-IU1--070420/638
Session Fixation	16-03-2020	7.5	TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier does not properly manage sessions, which allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5543**	N/A	O-MIT-IU1--070420/639
NULL Pointer Dereference	16-03-2020	7.5	Null Pointer Dereference vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier	N/A	O-MIT-IU1--070420/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5544**		
N/A	16-03-2020	7.5	TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to bypass access restriction and to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5545**	N/A	O-MIT-IU1--070420/641
Argument Injection or Modification	16-03-2020	5.8	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows an attacker on the same network segment to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5546**	N/A	O-MIT-IU1--070420/642
Improper Input Validation	16-03-2020	7.5	Resource Management Errors vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series	N/A	O-MIT-IU1--070420/643

CVSS 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
			IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5547**		
Motorola					
fx9500-41324d41-us_firmware					
Information Exposure	23-03-2020	5	Motorola FX9500 devices allow remote attackers to read database files. **CVE ID : CVE-2020-10874**	N/A	O-MOT-FX95-070420/644
fx9500-41324d41-ww_firmware					
Information Exposure	23-03-2020	5	Motorola FX9500 devices allow remote attackers to read database files. **CVE ID : CVE-2020-10874**	N/A	O-MOT-FX95-070420/645
fx9500-81324d41-us_firmware					
Information Exposure	23-03-2020	5	Motorola FX9500 devices allow remote attackers to read database files. **CVE ID : CVE-2020-10874**	N/A	O-MOT-FX95-070420/646
fx9500-81324d41-ww_firmware					
Information Exposure	23-03-2020	5	Motorola FX9500 devices allow remote attackers to read database files. **CVE ID : CVE-2020-10874**	N/A	O-MOT-FX95-070420/647
Moxa					
pt-7528-20msc-4tx-4gsfp-hv_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/648
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/649
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/650
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute	N/A	O-MOX-PT-7-070420/651

CVSS 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
			arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/652
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/653
pt-7528-8ssc-16tx-4gsfp-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/654
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/655

CVSS 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
			lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/656
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/657
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/658
Weak Password Requirement	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	O-MOX-PT-7-070420/659

CVSS 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
s			firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-8ssc-16tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/660
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/661
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/663
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/664
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/665
pt-7828-f-24_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which	N/A	O-MOX-PT-7-070420/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/667
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/668
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/669
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain	N/A	O-MOX-PT-7-070420/670

CVSS 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
			access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/671
pt-7828-f-24-24_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/672
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/673
Use of a Broken or Risky	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	O-MOX-PT-7-070420/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/675
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/676
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/677

CVSS 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
pt-7828-f-24-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/678
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/679
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/680
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service	N/A	O-MOX-PT-7-070420/681

CVSS 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
			condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/682
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/683
pt-7828-f-48_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/684
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	O-MOX-PT-7-070420/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/686
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/687
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/688
Weak Password	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Requirements			lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		070420/689
pt-7828-f-48-48_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/690
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/691
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed.	N/A	O-MOX-PT-7-070420/692

CVSS 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
			CVE ID : CVE-2020-6987		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/693
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/694
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/695
pt-7828-f-48-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded	N/A	O-MOX-PT-7-070420/696

CVSS 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
			cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/697
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/698
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/699
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/701
pt-7828-f-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/702
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/703
Use of a Broken or	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-070420/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Risky Cryptographic Algorithm			lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/705
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/706
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access.	N/A	O-MOX-PT-7-070420/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6995		
pt-7828-f-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/708
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/709
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/710
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause	N/A	O-MOX-PT-7-070420/711

CVSS 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
			a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/712
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/713
pt-7828-r-24_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/714
Use of Hard-coded	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-070420/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/716
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/717
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/718

CVSS 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
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/719
pt-7828-r-24-24_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/720
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/721
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information	N/A	O-MOX-PT-7-070420/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/723
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/724
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/725
pt-7828-r-24-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/727
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/728
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/729
Information	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-

CVSS 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
Exposure			lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		070420/730
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/731
pt-7828-r-48_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/732
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/733

CVSS 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
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/734
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/735
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/736
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may	N/A	O-MOX-PT-7-070420/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7828-r-48-48_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/738
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/739
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/740
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/741

CVSS 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
			lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/742
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/743
pt-7828-r-48-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered.	N/A	O-MOX-PT-7-070420/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6983		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/745
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/746
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/747
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without	N/A	O-MOX-PT-7-070420/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/749
pt-7828-r-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/750
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/751
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak	N/A	O-MOX-PT-7-070420/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/753
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/754
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/755
pt-7828-r-hv-hv_firmware					
Use of Hard-	24-03-2020	5	In Moxa PT-7528 series	N/A	O-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		070420/756
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/757
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/758
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code.	N/A	O-MOX-PT-7-070420/759

CVSS 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
			CVE ID : CVE-2020-6989		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/760
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/761
mds-g516e_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-03-2020	4	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, some of the parameters in the setting pages do not ensure text is the correct size for its buffer. **CVE ID : CVE-2020-6999**	N/A	O-MOX-MDS--070420/762
iologik_2512_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some	N/A	O-MOX-IOLO-070420/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web applications in clear text. **CVE ID : CVE-2020-7003**		
iologik_2512-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/764
iologik_2512-hspa_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/765
iologik_2512-hspa-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/766
iologik_2512-wl1-eu_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/767
iologik_2512-wl1-eu-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/768
iologik_2512-wl1-us_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/769
iologik_2512-wl1-us-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower,	N/A	O-MOX-IOLO-070420/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**		
pt-7528-12msc-12tx-4gsfp-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/771
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/772
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/773
Out-of-bounds	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-070420/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/775
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/776
pt-7528-16msc-8tx-4gsfp-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can	N/A	O-MOX-PT-7-070420/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/778
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/779
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/780
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web	N/A	O-MOX-PT-7-070420/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/782
pt-7528-12msc-12tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/783
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/784
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected	N/A	O-MOX-PT-7-070420/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/786
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/787
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/788
pt-7528-16msc-8tx-4gsfp-hv-hv_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/789
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/790
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/791
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute	N/A	O-MOX-PT-7-070420/792

CVSS 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
			arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/793
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/794
pt-7528-12msc-12tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/795
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/796

CVSS 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
			lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/797
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/798
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/799
Weak Password Requirement	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	O-MOX-PT-7-070420/800

CVSS 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
s			firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-16msc-8tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/801
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/802
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/804
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/805
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/806
pt-7528-12mst-12tx-4gsfp-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which	N/A	O-MOX-PT-7-070420/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/808
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/809
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/810
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain	N/A	O-MOX-PT-7-070420/811

CVSS 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
			access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/812
pt-7528-16msc-8tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/813
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/814
Use of a Broken or Risky	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	O-MOX-PT-7-070420/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/816
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/817
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/818

CVSS 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
eds-g516e_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a hard-coded cryptographic key, increasing the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6979**	N/A	O-MOX-EDS--070420/819
Use of Hard-coded Credentials	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, an attacker may gain access to the system without proper authentication. **CVE ID : CVE-2020-6981**	N/A	O-MOX-EDS--070420/820
Weak Password Requirements	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, weak password requirements may allow an attacker to gain access using brute force. **CVE ID : CVE-2020-6991**	N/A	O-MOX-EDS--070420/821
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, sensitive information is transmitted over some web applications in cleartext. **CVE ID : CVE-2020-6997**	N/A	O-MOX-EDS--070420/822
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information	N/A	O-MOX-EDS--070420/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to be disclosed. **CVE ID : CVE-2020-7001**		
Out-of-bounds Write	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the attacker may execute arbitrary codes or target the device, causing it to go out of service. **CVE ID : CVE-2020-7007**	N/A	O-MOX-EDS--070420/824
pt-7528-12mst-12tx-4gsfp-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/825
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/826
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information	N/A	O-MOX-PT-7-070420/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/828
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/829
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/830
pt-7528-16mst-8tx-4gsfp-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/832
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/833
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/834
Information	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		070420/835
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/836
pt-7528-16mst-8tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/837
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/839
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/840
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/841
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may	N/A	O-MOX-PT-7-070420/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-20msc-4tx-4gsfp-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/843
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/844
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/845
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/847
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/848
pt-7528-20mst-4tx-4gsfp-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered.	N/A	O-MOX-PT-7-070420/849

CVSS 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
			CVE ID : CVE-2020-6983		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/850
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/851
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/852
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without	N/A	O-MOX-PT-7-070420/853

CVSS 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
			authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/854
pt-7528-20msc-4tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/855
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/856
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak	N/A	O-MOX-PT-7-070420/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/858
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/859
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/860
pt-7528-20mst-4tx-4gsfp-hv-hv_firmware					
Use of Hard-	24-03-2020	5	In Moxa PT-7528 series	N/A	O-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		070420/861
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/862
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/863
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code.	N/A	O-MOX-PT-7-070420/864

CVSS 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
			CVE ID : CVE-2020-6989		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/865
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/866
pt-7528-20msc-4tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/867
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code	N/A	O-MOX-PT-7-070420/868

CVSS 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
			for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/869
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/870
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/871
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application	N/A	O-MOX-PT-7-070420/872

CVSS 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
			utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-8mst-16tx-4gsfp-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/873
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/874
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/875
Out-of-bounds	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-070420/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/877
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/878
pt-7528-12mst-12tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can	N/A	O-MOX-PT-7-070420/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/880
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/881
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/882
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web	N/A	O-MOX-PT-7-070420/883

CVSS 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 without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/884
pt-7528-16mst-8tx-4gsfp-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/885
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/886
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected	N/A	O-MOX-PT-7-070420/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/888
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/889
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/890
pt-7528-8msc-16tx-4gsfp-wv-wv_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/891
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/892
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/893
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute	N/A	O-MOX-PT-7-070420/894

CVSS 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
			arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/895
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/896
pt-7528-8mst-16tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/897
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/898

CVSS 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
			lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/899
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/900
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/901
Weak Password Requirement	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	O-MOX-PT-7-070420/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
s			firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-12mst-12tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/903
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/904
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/906
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/907
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/908
pt-7528-16mst-8tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which	N/A	O-MOX-PT-7-070420/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/910
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/911
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/912
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain	N/A	O-MOX-PT-7-070420/913

CVSS 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
			access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/914
iologik_2512-wl1-jp_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/915
iologik_2512-wl1-jp-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/916
iologik_2542_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/917
iologik_2542-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/918
iologik_2542-hspa_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/919
iologik_2542-hspa-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower,	N/A	O-MOX-IOLO-070420/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**		
iologik_2542-wl1-eu_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/921
iologik_2542-wl1-eu-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/922
iologik_2542-wl1-us_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/923

CVSS 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
iologik_2542-wl1-us-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/924
iologik_2542-wl1-jp_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/925
iologik_2542-wl1-jp-t_firmware					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	O-MOX-IOLO-070420/926
pt-7528-8msc-16tx-4gsfp-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/928
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/929
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/930
Information	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-

CVSS 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
Exposure			lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		070420/931
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/932
pt-7528-20mst-4tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/933
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/934

CVSS 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
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/935
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/936
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/937
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may	N/A	O-MOX-PT-7-070420/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-8msc-16tx-4gsfp-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/939
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/940
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/941
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/942

CVSS 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
			lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/943
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/944
pt-7528-20mst-4tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered.	N/A	O-MOX-PT-7-070420/945

CVSS 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
			CVE ID : CVE-2020-6983		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/946
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/947
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/948
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without	N/A	O-MOX-PT-7-070420/949

CVSS 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
			authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/950
pt-7528-8mst-16tx-4gsfp-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/951
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/952
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak	N/A	O-MOX-PT-7-070420/953

CVSS 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
			cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/954
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/955
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/956
pt-7528-8mst-16tx-4gsfp-hv_firmware					
Use of Hard-	24-03-2020	5	In Moxa PT-7528 series	N/A	O-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		070420/957
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/958
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/959
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code.	N/A	O-MOX-PT-7-070420/960

CVSS 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
			CVE ID : CVE-2020-6989		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/961
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/962
pt-7528-8msc-16tx-4gsfp-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/963
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code	N/A	O-MOX-PT-7-070420/964

CVSS 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
			for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/965
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/966
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/967
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application	N/A	O-MOX-PT-7-070420/968

CVSS 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
			utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
eds-510e_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a hard-coded cryptographic key, increasing the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6979**	N/A	O-MOX-EDS--070420/969
Use of Hard-coded Credentials	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, an attacker may gain access to the system without proper authentication. **CVE ID : CVE-2020-6981**	N/A	O-MOX-EDS--070420/970
Weak Password Requirements	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, weak password requirements may allow an attacker to gain access using brute force. **CVE ID : CVE-2020-6991**	N/A	O-MOX-EDS--070420/971
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, sensitive information is transmitted over some web applications in cleartext. **CVE ID : CVE-2020-6997**	N/A	O-MOX-EDS--070420/972
Use of a Broken or	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or	N/A	O-MOX-EDS--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Risky Cryptographic Algorithm			lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-7001**		070420/973
Out-of-bounds Write	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the attacker may execute arbitrary codes or target the device, causing it to go out of service. **CVE ID : CVE-2020-7007**	N/A	O-MOX-EDS--070420/974
pt-7528-24tx-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/975
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/976
Use of a Broken or Risky Cryptographi	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Algorithm			lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/978
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/979
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/980

CVSS 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
pt-7528-24tx-hv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/981
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/982
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/983
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service	N/A	O-MOX-PT-7-070420/984

CVSS 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
			condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/985
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/986
pt-7528-24tx-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/987
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	O-MOX-PT-7-070420/988

CVSS 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
			firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/989
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/990
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/991
Weak Password	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Requirements			lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		070420/992
pt-7528-24tx-wv-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/993
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/994
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed.	N/A	O-MOX-PT-7-070420/995

CVSS 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
			CVE ID : CVE-2020-6987		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/996
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/997
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/998
pt-7528-24tx-wv-wv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded	N/A	O-MOX-PT-7-070420/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/1000
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	O-MOX-PT-7-070420/1001
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/1002
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	O-MOX-PT-7-070420/1003

CVSS 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
			lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	O-MOX-PT-7-070420/1004
pt-7528-12msc-12tx-4gsfp-hv_firmware					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	O-MOX-PT-7-070420/1005
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	O-MOX-PT-7-070420/1006
Use of a Broken or	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	O-MOX-PT-7-070420/1007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Risky Cryptographic Algorithm			lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	O-MOX-PT-7-070420/1008
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	O-MOX-PT-7-070420/1009
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access.	N/A	O-MOX-PT-7-070420/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6995		
Redhat					
virtualization					
Missing Authorization	17-03-2020	3.5	A flaw was found in PostgreSQL's "ALTER ... DEPENDS ON EXTENSION", where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2, before 11.7, before 10.12 and before 9.6.17. **CVE ID : CVE-2020-1720**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1720	O-RED-VIRT-070420/1011
enterprise_linux					
Missing Authorization	17-03-2020	3.5	A flaw was found in PostgreSQL's "ALTER ... DEPENDS ON EXTENSION", where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2,	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1720	O-RED-ENTE-070420/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 11.7, before 10.12 and before 9.6.17. **CVE ID : CVE-2020-1720**		
Rockwellautomation					
micrologix_1100_firmware					
Cleartext Storage of Sensitive Information	16-03-2020	2.1	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext. **CVE ID : CVE-2020-6980**	N/A	O-ROC-MICR-070420/1013
Use of a Broken or Risky Cryptographic Algorithm	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic function utilized to protect the password in MicroLogix is discoverable. **CVE ID : CVE-2020-6984**	N/A	O-ROC-MICR-070420/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials. **CVE ID : CVE-2020-6988**	N/A	O-ROC-MICR-070420/1015
Use of Hard-coded Credentials	16-03-2020	10	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and	N/A	O-ROC-MICR-070420/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller. **CVE ID : CVE-2020-6990**		
micrologix_1400_a_firmware					
Cleartext Storage of Sensitive Information	16-03-2020	2.1	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext. **CVE ID : CVE-2020-6980**	N/A	O-ROC-MICR-070420/1017
Use of a Broken or Risky Cryptographic Algorithm	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic function utilized to protect the password in MicroLogix is	N/A	O-ROC-MICR-070420/1018

CVSS 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
			discoverable. **CVE ID : CVE-2020-6984**		
Improper Authentication	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials. **CVE ID : CVE-2020-6988**	N/A	O-ROC-MICR-070420/1019
Use of Hard-coded Credentials	16-03-2020	10	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect the account password is hard coded into the	N/A	O-ROC-MICR-070420/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller. **CVE ID : CVE-2020-6990**		
micrologix_1400_b_firmware					
Cleartext Storage of Sensitive Information	16-03-2020	2.1	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext. **CVE ID : CVE-2020-6980**	N/A	O-ROC-MICR-070420/1021
Use of a Broken or Risky Cryptographic Algorithm	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic function utilized to protect	N/A	O-ROC-MICR-070420/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the password in MicroLogix is discoverable. **CVE ID : CVE-2020-6984**		
Improper Authenticati on	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials. **CVE ID : CVE-2020-6988**	N/A	O-ROC-MICR-070420/1023
Use of Hard-coded Credentials	16-03-2020	10	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect	N/A	O-ROC-MICR-070420/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller. **CVE ID : CVE-2020-6990**		
Schneider-electric					
tsxp57254m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-TSXP-070420/1025
tsxp572634m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet	N/A	O-SCH-TSXP-070420/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp57204m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-TSXP-070420/1027
tsxp571634m_firmware					
Improper Check for Unusual or Exceptional	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in	N/A	O-SCH-TSXP-070420/1028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp57154m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-TSXP-070420/1029
tsxp57104m_firmware					
Improper Check for Unusual or	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions	N/A	O-SCH-TSXP-070420/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140cpu65150_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140C-070420/1031
140cpu65160_firmware					
Improper Check for	23-03-2020	5	A CWE-754: Improper Check for Unusual or	N/A	O-SCH-140C-070420/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140cpu65260_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140C-070420/1033
140cpu67261_firmware					
Improper	23-03-2020	5	A CWE-754: Improper	N/A	O-SCH-140C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Unusual or Exceptional Conditions			Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		070420/1034
140cpu67060_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140C-070420/1035
140cpu67160_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140C-070420/1036
140cpu67260_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140C-070420/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
140cpu65860_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140C-070420/1038
140cpu67861_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus.	N/A	O-SCH-140C-070420/1039

CVSS 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
			CVE ID : CVE-2020-7477		
140cpu65160s_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140C-070420/1040
140cpu67160s_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command	N/A	O-SCH-140C-070420/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over Modbus. **CVE ID : CVE-2020-7477**		
modicon_m340_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-03-2020	7.5	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), reflective DLL, vulnerability exists in EcoStruxure Control Expert (all versions prior to 14.1 Hot Fix), Unity Pro (all versions), Modicon M340 (all versions prior to V3.20), Modicon M580 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller. **CVE ID : CVE-2020-7475**	N/A	O-SCH-MODI-070420/1042
140noe77101_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a	N/A	O-SCH-140N-070420/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140noe77111_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-140N-070420/1044
tsxh5744m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial	N/A	O-SCH-TSXH-070420/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxh5724m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-TSXH-070420/1046
tsxp576634m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions),	N/A	O-SCH-TSXP-070420/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp57554m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-TSXP-070420/1048
tsxp575634m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated	N/A	O-SCH-TSXP-070420/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp57454m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-TSXP-070420/1050
tsxp574634m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium	N/A	O-SCH-TSXP-070420/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp573634m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	O-SCH-TSXP-070420/1052
tsxp57304m_firmware					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all	N/A	O-SCH-TSXP-070420/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
modicon_m580_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-03-2020	7.5	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), reflective DLL, vulnerability exists in EcoStruxure Control Expert (all versions prior to 14.1 Hot Fix), Unity Pro (all versions), Modicon M340 (all versions prior to V3.20), Modicon M580 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller. **CVE ID : CVE-2020-7475**	N/A	O-SCH-MODI-070420/1054
andover_continuum_9680_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1056
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1057
andover_continuum_5740_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1059
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1060
andover_continuum_5720_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1062
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1063
andover_continuum_bcx4040_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1065
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1066
andover_continuum_bcx9640_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1068
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1069
andover_continuum_9900_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1071
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1072
andover_continuum_9940_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1074
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1075
andover_continuum_9941_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1077
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1078
andover_continuum_9924_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1080
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1081
andover_continuum_9702_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1083
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1084
andover_continuum_9200_firmware					
Improper Control of Generation of Code ('Code Injection')	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker	N/A	O-SCH-ANDO-070420/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	O-SCH-ANDO-070420/1086
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	O-SCH-ANDO-070420/1087
Sonicwall					
sma1000_firmware					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	26-03-2020	5	A vulnerability in the SonicWall SMA1000 HTTP Extraweb server allows an unauthenticated remote attacker to cause HTTP server crash which leads to Denial of Service. This vulnerability affected SMA1000 Version 12.1.0-	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0002	O-SON-SMA1-070420/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			06411 and earlier. **CVE ID : CVE-2020-5129**		
Suse					
suse_linux_enterprise_server					
Use After Free	23-03-2020	9.3	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6422**	N/A	O-SUS-SUSE-070420/1089
Use After Free	23-03-2020	9.3	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6424**	N/A	O-SUS-SUSE-070420/1090
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-03-2020	4.3	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6426**	N/A	O-SUS-SUSE-070420/1091
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6427**	N/A	O-SUS-SUSE-070420/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6428**	N/A	O-SUS-SUSE-070420/1093
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6429**	N/A	O-SUS-SUSE-070420/1094
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6449**	N/A	O-SUS-SUSE-070420/1095
suse_linux_enterprise_desktop					
Use After Free	23-03-2020	9.3	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6422**	N/A	O-SUS-SUSE-070420/1096
Use After Free	23-03-2020	9.3	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap	N/A	O-SUS-SUSE-070420/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption via a crafted HTML page. **CVE ID : CVE-2020-6424**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-03-2020	4.3	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6426**	N/A	O-SUS-SUSE-070420/1098
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6427**	N/A	O-SUS-SUSE-070420/1099
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6428**	N/A	O-SUS-SUSE-070420/1100
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6429**	N/A	O-SUS-SUSE-070420/1101
Use After Free	23-03-2020	9.3	Use after free in audio in Google Chrome prior to	N/A	O-SUS-SUSE-070420/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6449**		
Systech					
nds\/5008rm_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	6	Systech Corporation NDS-5000 Terminal Server, NDS/5008 (8 Port, RJ45), firmware Version 02D.30. Successful exploitation of this vulnerability could allow information disclosure, limit system availability, and may allow remote code execution. **CVE ID : CVE-2020-7006**	N/A	O-SYS-NDS\-070420/1103
nds-5000_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	6	Systech Corporation NDS-5000 Terminal Server, NDS/5008 (8 Port, RJ45), firmware Version 02D.30. Successful exploitation of this vulnerability could allow information disclosure, limit system availability, and may allow remote code execution. **CVE ID : CVE-2020-7006**	N/A	O-SYS-NDS--070420/1104
zebra					
fx9500_firmware					
Improper Limitation of a Pathname to a Restricted	23-03-2020	5	Motorola FX9500 devices allow remote attackers to conduct absolute path traversal attacks, as demonstrated by PL/SQL	N/A	O-ZEB-FX95-070420/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			Server Pages files such as /include/viewtagdb.psp. **CVE ID : CVE-2020-10875**		
Hardware					
Canon					
oce_colorwave_500					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	4.3	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Stored XSS in /TemplateManager/indexExternalLocation.jsp. The vulnerable parameter is map(template_name). NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10667**	N/A	H-CAN-OCE_-070420/1106
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	4.3	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Reflected XSS in /home.jsp. The vulnerable parameter is openSI. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10668**	N/A	H-CAN-OCE_-070420/1107
Improper Authentication	19-03-2020	5	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to authentication bypass on the page /home.jsp. An unauthenticated attacker	N/A	H-CAN-OCE_-070420/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			able to connect to the device's web interface can get a copy of the documents uploaded by any users. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10669**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	4.3	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Reflected XSS in the parameter settingId of the settingDialogContent.jsp page. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10670**	N/A	H-CAN-OCE_-070420/1109
Cross-Site Request Forgery (CSRF)	19-03-2020	6.8	The Canon Oce Colorwave 500 4.0.0.0 printer's web application is missing any form of CSRF protections. This is a system-wide issue. An attacker could perform administrative actions by targeting a logged-in administrative user. NOTE: this is fixed in the latest version. **CVE ID : CVE-2020-10671**	N/A	H-CAN-OCE_-070420/1110
Cisco					
isr1100-4g					
Buffer Copy without Checking Size of Input ('Classic	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer	N/A	H-CIS-ISR1-070420/1111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**		
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**	N/A	H-CIS-ISR1-070420/1112
Improper Neutralization of Special Elements used in an OS Command	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are	N/A	H-CIS-ISR1-070420/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**		
vedge_100					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**	N/A	H-CIS-VEDG-070420/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**	N/A	H-CIS-VEDG-070420/1115
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root	N/A	H-CIS-VEDG-070420/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-3266**		
vedge_1000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**	N/A	H-CIS-VEDG-070420/1117
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain	N/A	H-CIS-VEDG-070420/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			root-level privileges. **CVE ID : CVE-2020-3265**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**	N/A	H-CIS-VEDG-070420/1119
vedge_2000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A	N/A	H-CIS-VEDG-070420/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**		
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**	N/A	H-CIS-VEDG-070420/1121
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the	N/A	H-CIS-VEDG-070420/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**		
vedge_5000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**	N/A	H-CIS-VEDG-070420/1123
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability	N/A	H-CIS-VEDG-070420/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**	N/A	H-CIS-VEDG-070420/1125
vedge_100m					
Buffer Copy without Checking Size of Input ('Classic	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer	N/A	H-CIS-VEDG-070420/1126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**		
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**	N/A	H-CIS-VEDG-070420/1127
Improper Neutralization of Special Elements used in an OS Command	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are	N/A	H-CIS-VEDG-070420/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**		
vedge_100wm					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**	N/A	H-CIS-VEDG-070420/1129

CVSS 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
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**	N/A	H-CIS-VEDG-070420/1130
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root	N/A	H-CIS-VEDG-070420/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-3266**		
isr1100-4gltegb					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**	N/A	H-CIS-ISR1-070420/1132
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain	N/A	H-CIS-ISR1-070420/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			root-level privileges. **CVE ID : CVE-2020-3265**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**	N/A	H-CIS-ISR1-070420/1134
isr1100-4gltena					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A	N/A	H-CIS-ISR1-070420/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**		
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**	N/A	H-CIS-ISR1-070420/1136
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the	N/A	H-CIS-ISR1-070420/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**		
isr1100-6g					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**	N/A	H-CIS-ISR1-070420/1138
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability	N/A	H-CIS-ISR1-070420/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**	N/A	H-CIS-ISR1-070420/1140
vedge_100b					
Buffer Copy without Checking Size of Input ('Classic	19-03-2020	6.6	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer	N/A	H-CIS-VEDG-070420/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make. **CVE ID : CVE-2020-3264**		
Improper Privilege Management	19-03-2020	7.2	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges. **CVE ID : CVE-2020-3265**	N/A	H-CIS-VEDG-070420/1142
Improper Neutralization of Special Elements used in an OS Command	19-03-2020	7.2	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are	N/A	H-CIS-VEDG-070420/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3266**		
Dlink					
dir-878					
Improper Authentication	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper implementation of the authentication algorithm. An attacker can leverage this vulnerability to escalate privileges and	N/A	H-DLI-DIR--070420/1144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the router. Was ZDI-CAN-9470. **CVE ID : CVE-2020-8863**		
Incorrect Comparison	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of empty passwords. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9471. **CVE ID : CVE-2020-8864**	N/A	H-DLI-DIR--070420/1145
dir-882					
Improper Authentication	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the	N/A	H-DLI-DIR--070420/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of HNAP login requests. The issue results from the lack of proper implementation of the authentication algorithm. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-9470. **CVE ID : CVE-2020-8863**		
Incorrect Comparison	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of empty passwords. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9471. **CVE ID : CVE-2020-8864**	N/A	H-DLI-DIR--070420/1147
dir-867					
Improper Authenticati on	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected	N/A	H-DLI-DIR--070420/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper implementation of the authentication algorithm. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-9470. **CVE ID : CVE-2020-8863**		
Incorrect Comparison	23-03-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of empty passwords. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-	N/A	H-DLI-DIR--070420/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9471. **CVE ID : CVE-2020-8864**		
Draytek					
vigor2960					
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi through ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 2 of 3). **CVE ID : CVE-2020-10824**	N/A	H-DRA-VIGO-070420/1150
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi while base64 decoding ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 3 of 3). **CVE ID : CVE-2020-10825**	N/A	H-DRA-VIGO-070420/1151
Improper Neutralization of Special Elements used in an OS Command ('OS Command	26-03-2020	10	/cgi-bin/activate.cgi on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve command injection via a remote HTTP request in DEBUG	N/A	H-DRA-VIGO-070420/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			mode. **CVE ID : CVE-2020-10826**		
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in apmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10827**	N/A	H-DRA-VIGO-070420/1153
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in cvmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10828**	N/A	H-DRA-VIGO-070420/1154
vigor300b					
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi through ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 2 of 3). **CVE ID : CVE-2020-10824**	N/A	H-DRA-VIGO-070420/1155
Out-of-	26-03-2020	7.5	A stack-based buffer	N/A	H-DRA-VIGO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			overflow in /cgi-bin/activate.cgi while base64 decoding ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 3 of 3). **CVE ID : CVE-2020-10825**		070420/1156
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-03-2020	10	/cgi-bin/activate.cgi on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve command injection via a remote HTTP request in DEBUG mode. **CVE ID : CVE-2020-10826**	N/A	H-DRA-VIGO-070420/1157
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in apmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10827**	N/A	H-DRA-VIGO-070420/1158
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in cvmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows	N/A	H-DRA-VIGO-070420/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10828**		
vigor3900					
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi through ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 2 of 3). **CVE ID : CVE-2020-10824**	N/A	H-DRA-VIGO-070420/1160
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in /cgi-bin/activate.cgi while base64 decoding ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 3 of 3). **CVE ID : CVE-2020-10825**	N/A	H-DRA-VIGO-070420/1161
Improper Neutralization of Special Elements used in an OS Command	26-03-2020	10	/cgi-bin/activate.cgi on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve command	N/A	H-DRA-VIGO-070420/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			injection via a remote HTTP request in DEBUG mode. **CVE ID : CVE-2020-10826**		
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in apmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10827**	N/A	H-DRA-VIGO-070420/1163
Out-of-bounds Write	26-03-2020	7.5	A stack-based buffer overflow in cvmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request. **CVE ID : CVE-2020-10828**	N/A	H-DRA-VIGO-070420/1164
Grandstream					
ucm6204					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1165

CVSS 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
			CVE ID : CVE-2020-5724		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	4.3	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords. **CVE ID : CVE-2020-5725**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1166
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5726**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1167
ucm6200					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-03-2020	10	The HTTP interface of the Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via crafted HTTP request. An attacker can use this vulnerability to execute shell commands as root on versions before 1.0.19.20 or inject HTML in password recovery emails in versions before 1.0.20.17.	N/A	H-GRA-UCM6-070420/1168

CVSS 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
			CVE ID : CVE-2020-5722		
ucm6202					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5724**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1169
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	4.3	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords. **CVE ID : CVE-2020-5725**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1170
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5726**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ucm6208					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5724**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1172
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	4.3	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords. **CVE ID : CVE-2020-5725**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1173
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-03-2020	5	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords. **CVE ID : CVE-2020-5726**	https://www.tenable.com/security/research/tra-2020-17	H-GRA-UCM6-070420/1174
Huawei					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mate_30_pro					
Improper Authentication	20-03-2020	2.1	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1793**	N/A	H-HUA-MATE-070420/1175
Improper Authentication	20-03-2020	2.1	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro	N/A	H-HUA-MATE-070420/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions Versions earlier than 10.0.0.203(C00E202R7P2) . **CVE ID : CVE-2020-1794**		
N/A	20-03-2020	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2) . **CVE ID : CVE-2020-1795**	N/A	H-HUA-MATE-070420/1177
Incorrect Authorization	20-03-2020	4.6	There is an improper authorization vulnerability in several smartphones. The software incorrectly performs an authorization to certain user, successful exploit could allow a low privilege user to do certain operation which the user are supposed not to do.Affected product	N/A	H-HUA-MATE-070420/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2) . **CVE ID : CVE-2020-1796**		
oxfords-an00a					
Improper Authentication	20-03-2020	2.1	Huawei smartphone OxfordS-AN00A with versions earlier than 10.0.1.152D(C735E152R3P3),versions earlier than 10.0.1.160(C00E160R4P1) have an improper authentication vulnerability. Authentication to target component is improper when device performs an operation. Attackers exploit this vulnerability to obtain some information by loading malicious application, leading to information leak. **CVE ID : CVE-2020-1878**	N/A	H-HUA-OXFO-070420/1179
oxfordp-an10b					
Improper Authentication	26-03-2020	6.8	Huawei smartphones OxfordP-AN10B with versions earlier than 10.0.1.169(C00E166R4P1) have an improper authentication vulnerability. The	N/A	H-HUA-OXFO-070420/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Application doesn't perform proper authentication when user performs certain operations. An attacker can trick user into installing a malicious plug-in to exploit this vulnerability. Successful exploit could allow the attacker to bypass the authentication to perform unauthorized operations. **CVE ID : CVE-2020-9066**		
taurus-al00b					
Use After Free	26-03-2020	2.1	Huawei smart phone Taurus-AL00B with versions earlier than 10.0.0.203(C00E201R7P2) have a use-after-free (UAF) vulnerability. An authenticated, local attacker may perform specific operations to exploit this vulnerability. Successful exploitation may tamper with the information to affect the availability. **CVE ID : CVE-2020-9065**	N/A	H-HUA-TAUR-070420/1181
secospace_antiddos8000					
Improper Authentication	20-03-2020	6.8	Some Huawei products have a security vulnerability due to improper authentication. A remote attacker needs to obtain some information and forge the peer device to send specific packets to	N/A	H-HUA-SECO-070420/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device. Due to the improper implementation of the authentication function, attackers can exploit the vulnerability to connect to affected devices and execute a series of commands.Affected product versions include:Secospace AntiDDoS8000 versions V500R001C00,V500R001C20,V500R001C60,V500R005C00. **CVE ID : CVE-2020-1864**		
p30					
Incorrect Authorization	26-03-2020	6.8	HUAWEI smartphones P30 with versions earlier than 10.0.0.185(C00E85R1P11) have an improper access control vulnerability. The software incorrectly restricts access to a function interface from an unauthorized actor, the attacker tricks the user into installing a crafted application, successful exploit could allow the attacker do certain unauthenticated operations. **CVE ID : CVE-2020-1800**	N/A	H-HUA-P30-070420/1183
mate_20					
Improper Authentication	20-03-2020	2.1	There is an improper authentication vulnerability in several	N/A	H-HUA-MATE-070420/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1793**		
Improper Authentication	20-03-2020	2.1	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2).	N/A	H-HUA-MATE-070420/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1794		
N/A	20-03-2020	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8); HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1795**	N/A	H-HUA-MATE-070420/1186
Incorrect Authorization	20-03-2020	4.6	There is an improper authorization vulnerability in several smartphones. The software incorrectly performs an authorization to certain user, successful exploit could allow a low privilege user to do certain operation which the user are supposed not to do.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8);	N/A	H-HUA-MATE-070420/1187

CVSS 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
			HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2). **CVE ID : CVE-2020-1796**		
osca-550					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**	N/A	H-HUA-OSCA-070420/1188
osca-550a					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper	N/A	H-HUA-OSCA-070420/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**		
osca-550ax					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions	N/A	H-HUA-OSCA-070420/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**		
osca-550x					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**	N/A	H-HUA-OSCA-070420/1191
hege-560					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may	N/A	H-HUA-HEGE-070420/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**		
hege-570					
Improper Validation of Integrity Check Value	20-03-2020	3.6	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-	N/A	H-HUA-HEGE-070420/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3). **CVE ID : CVE-2020-1879**		
insulet					
omnipod_insulin_management_system					
Incorrect Authorization	20-03-2020	4.6	The affected insulin pump is designed to communicate using a wireless RF with an Insulet manufactured Personal Diabetes Manager device. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with access to one of the affected insulin pump models may be able to modify and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery. **CVE ID : CVE-2020-10597**	N/A	H-INS-OMNI-070420/1194
Mikrotik					
ccr1009-7g-1c-1s\+					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via	N/A	H-MIK-CCR1-070420/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
ccr1009-7g-1c-1s\+pc					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-CCR1-070420/1196
ccr1009-7g-1c-pc					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-CCR1-070420/1197
ccr1016-12g					
Uncontrolled	23-03-2020	5	The SSH daemon on	N/A	H-MIK-CCR1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		070420/1198
ccr1016-12s-1s\+					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-CCR1-070420/1199
ccr1036-12g-4s					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of	N/A	H-MIK-CCR1-070420/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uncontrolled resource management. **CVE ID : CVE-2020-10364**		
ccr1036-12g-4s-em					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-CCR1-070420/1201
ccr1036-8g-2s\+					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-CCR1-070420/1202
ccr1036-8g-2s\+em					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow	N/A	H-MIK-CCR1-070420/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
ccr1072-1g-8s\+					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-CCR1-070420/1204
hex					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management.	N/A	H-MIK-HEX-070420/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10364		
hex_lite					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-HEX_-070420/1206
hex_poe					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-HEX_-070420/1207
hex_poe_lite					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new	N/A	H-MIK-HEX_-070420/1208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
hex_s					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-HEX_-070420/1209
powerbox					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-POWE-070420/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
powerbox_pro					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-POWE-070420/1211
rb1100ahx4					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-RB11-070420/1212
rb2011il-in					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via	N/A	H-MIK-RB20-070420/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		
rb2011il-rm					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-RB20-070420/1214
rb2011ils-in					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-RB20-070420/1215
rb2011uias-in					
Uncontrolled	23-03-2020	5	The SSH daemon on	N/A	H-MIK-RB20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**		070420/1216
rb2011uias-rm					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-RB20-070420/1217
rb3011uias-rm					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of	N/A	H-MIK-RB30-070420/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uncontrolled resource management. **CVE ID : CVE-2020-10364**		
rb4011igs\+rm					
Uncontrolled Resource Consumption	23-03-2020	5	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management. **CVE ID : CVE-2020-10364**	N/A	H-MIK-RB40-070420/1219
Mitsubishielectric					
iu1-1m20-d					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-03-2020	7.5	Buffer error vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5542**	N/A	H-MIT-IU1--070420/1220
Session Fixation	16-03-2020	7.5	TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier	N/A	H-MIT-IU1--070420/1221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not properly manage sessions, which allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5543**		
NULL Pointer Dereference	16-03-2020	7.5	Null Pointer Dereference vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5544**	N/A	H-MIT-IU1--070420/1222
N/A	16-03-2020	7.5	TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to bypass access restriction and to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5545**	N/A	H-MIT-IU1--070420/1223
Argument Injection or Modification	16-03-2020	5.8	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series	N/A	H-MIT-IU1--070420/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IU1-1M20-D firmware version 1.0.7 and earlier allows an attacker on the same network segment to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5546**		
Improper Input Validation	16-03-2020	7.5	Resource Management Errors vulnerability in TCP function included in the firmware of Mitsubishi Electric MELQIC IU1 series IU1-1M20-D firmware version 1.0.7 and earlier allows remote attackers to stop the network functions or execute malware via a specially crafted packet. **CVE ID : CVE-2020-5547**	N/A	H-MIT-IU1--070420/1225
Motorola					
fx9500-41324d41-us					
Information Exposure	23-03-2020	5	Motorola FX9500 devices allow remote attackers to read database files. **CVE ID : CVE-2020-10874**	N/A	H-MOT-FX95-070420/1226
fx9500-41324d41-ww					
Information Exposure	23-03-2020	5	Motorola FX9500 devices allow remote attackers to read database files. **CVE ID : CVE-2020-10874**	N/A	H-MOT-FX95-070420/1227
fx9500-81324d41-us					
Information	23-03-2020	5	Motorola FX9500 devices	N/A	H-MOT-FX95-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			allow remote attackers to read database files. **CVE ID : CVE-2020-10874**		070420/1228
fx9500-81324d41-ww					
Information Exposure	23-03-2020	5	Motorola FX9500 devices allow remote attackers to read database files. **CVE ID : CVE-2020-10874**	N/A	H-MOT-FX95-070420/1229
Moxa					
pt-7528-16mst-8tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1230
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1231
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm,	N/A	H-MOX-PT-7-070420/1232

CVSS 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
			which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1233
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1234
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1235
pt-7528-20msc-4tx-4gsfp-hv					
Use of Hard-coded	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	H-MOX-PT-7-070420/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1237
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1238
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1239

CVSS 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
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1240
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1241
pt-7528-8mst-16tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1242
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console.	N/A	H-MOX-PT-7-070420/1243

CVSS 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
			CVE ID : CVE-2020-6985		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1244
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1245
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1246
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password	N/A	H-MOX-PT-7-070420/1247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-8ssc-16tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1248
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1249
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1250
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1252
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1253
pt-7528-8ssc-16tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered.	N/A	H-MOX-PT-7-070420/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6983		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1255
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1256
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1257
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without	N/A	H-MOX-PT-7-070420/1258

CVSS 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
			authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1259
pt-7828-f-24					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1260
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1261
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak	N/A	H-MOX-PT-7-070420/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1263
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1264
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1265
pt-7828-f-24-24					
Use of Hard-	24-03-2020	5	In Moxa PT-7528 series	N/A	H-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		070420/1266
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1267
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1268
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code.	N/A	H-MOX-PT-7-070420/1269

CVSS 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
			CVE ID : CVE-2020-6989		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1270
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1271
pt-7828-f-24-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1272
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code	N/A	H-MOX-PT-7-070420/1273

CVSS 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
			for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1274
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1275
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1276
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application	N/A	H-MOX-PT-7-070420/1277

CVSS 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
			utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7828-f-48					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1278
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1279
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1280
Out-of-bounds	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	H-MOX-PT-7-070420/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1282
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1283
pt-7828-f-48-48					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can	N/A	H-MOX-PT-7-070420/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1285
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1286
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1287
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web	N/A	H-MOX-PT-7-070420/1288

CVSS 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 without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1289
pt-7828-f-48-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1290
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1291
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected	N/A	H-MOX-PT-7-070420/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1293
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1294
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1295
pt-7828-f-hv					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1296
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1297
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1298
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute	N/A	H-MOX-PT-7-070420/1299

CVSS 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
			arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1300
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1301
pt-7828-f-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1302
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	H-MOX-PT-7-070420/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1304
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1305
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1306
Weak Password Requirement	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1307

CVSS 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
s			firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7828-r-24					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1308
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1309
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1311
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1312
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1313
pt-7828-r-24-24					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which	N/A	H-MOX-PT-7-070420/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1315
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1316
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1317
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain	N/A	H-MOX-PT-7-070420/1318

CVSS 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
			access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1319
pt-7828-r-24-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1320
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1321
Use of a Broken or Risky	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1322

CVSS 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
Cryptographic Algorithm			firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1323
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1324
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pt-7828-r-48					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1326
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1327
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1328
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service	N/A	H-MOX-PT-7-070420/1329

CVSS 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
			condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1330
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1331
pt-7828-r-48-48					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1332
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1334
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1335
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1336
Weak Password	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	H-MOX-PT-7-

CVSS 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
Requirements			lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		070420/1337
pt-7828-r-48-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1338
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1339
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed.	N/A	H-MOX-PT-7-070420/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6987		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1341
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1342
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1343
pt-7828-r-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded	N/A	H-MOX-PT-7-070420/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1345
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1346
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1347
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	H-MOX-PT-7-070420/1348

CVSS 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
			lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1349
pt-7828-r-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1350
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1351
Use of a Broken or	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	H-MOX-PT-7-070420/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Risky Cryptographic Algorithm			lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1353
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1354
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access.	N/A	H-MOX-PT-7-070420/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6995		
mds-g516e					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-03-2020	4	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, some of the parameters in the setting pages do not ensure text is the correct size for its buffer. **CVE ID : CVE-2020-6999**	N/A	H-MOX-MDS--070420/1356
iologik_2512					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1357
iologik_2512-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1358
iologik_2512-hspa					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower,	N/A	H-MOX-IOLO-070420/1359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**		
iologik_2512-hspa-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1360
iologik_2512-wl1-eu					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1361
iologik_2512-wl1-eu-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
iologik_2512-wl1-us					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1363
iologik_2512-wl1-us-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1364
pt-7528-12msc-12tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1365
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	H-MOX-PT-7-070420/1366

CVSS 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
			lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1367
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1368
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1369
Weak Password Requirement	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1370

CVSS 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
s			firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-16msc-8tx-4gsfp-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1371
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1372
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1374
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1375
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1376
pt-7528-12msc-12tx-4gsfp-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which	N/A	H-MOX-PT-7-070420/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1378
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1379
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1380
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain	N/A	H-MOX-PT-7-070420/1381

CVSS 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
			access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1382
pt-7528-16msc-8tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1383
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1384
Use of a Broken or Risky	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1386
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1387
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pt-7528-12msc-12tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1389
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1390
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1391
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service	N/A	H-MOX-PT-7-070420/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1393
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1394
pt-7528-16msc-8tx-4gsfp-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1395
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1397
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1398
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1399
Weak Password	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	H-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Requirements			lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		070420/1400
eds-g516e					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a hard-coded cryptographic key, increasing the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6979**	N/A	H-MOX-EDS--070420/1401
Use of Hard-coded Credentials	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, an attacker may gain access to the system without proper authentication. **CVE ID : CVE-2020-6981**	N/A	H-MOX-EDS--070420/1402
Weak Password Requirements	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, weak password requirements may allow an attacker to gain access using brute force. **CVE ID : CVE-2020-6991**	N/A	H-MOX-EDS--070420/1403
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, sensitive information is transmitted over some web applications in cleartext.	N/A	H-MOX-EDS--070420/1404

CVSS 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
			CVE ID : CVE-2020-6997		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-7001**	N/A	H-MOX-EDS--070420/1405
Out-of-bounds Write	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the attacker may execute arbitrary codes or target the device, causing it to go out of service. **CVE ID : CVE-2020-7007**	N/A	H-MOX-EDS--070420/1406
pt-7528-12mst-12tx-4gsfp-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1407
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1408
Use of a	24-03-2020	5	In Moxa PT-7528 series	N/A	H-MOX-PT-7-

CVSS 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
Broken or Risky Cryptographic Algorithm			firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		070420/1409
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1410
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1411
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain	N/A	H-MOX-PT-7-070420/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-16msc-8tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1413
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1414
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1415
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in	N/A	H-MOX-PT-7-070420/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1417
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1418
pt-7528-20msc-4tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1419

CVSS 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
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1420
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1421
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1422
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization.	N/A	H-MOX-PT-7-070420/1423

CVSS 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
			CVE ID : CVE-2020-6993		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1424
pt-7528-8mst-16tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1425
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1426
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow	N/A	H-MOX-PT-7-070420/1427

CVSS 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
			confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1428
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1429
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1430
pt-7528-12mst-12tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1432
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1433
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1434

CVSS 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
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1435
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1436
pt-7528-16mst-8tx-4gsfp-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1437
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console.	N/A	H-MOX-PT-7-070420/1438

CVSS 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
			CVE ID : CVE-2020-6985		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1439
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1440
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1441
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password	N/A	H-MOX-PT-7-070420/1442

CVSS 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
			requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-20mst-4tx-4gsfp-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1443
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1444
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1445
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1447
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1448
pt-7528-20msc-4tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered.	N/A	H-MOX-PT-7-070420/1449

CVSS 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
			CVE ID : CVE-2020-6983		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1450
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1451
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1452
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without	N/A	H-MOX-PT-7-070420/1453

CVSS 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
			authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1454
pt-7528-20mst-4tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1455
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1456
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak	N/A	H-MOX-PT-7-070420/1457

CVSS 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
			cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1458
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1459
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1460
pt-7528-12mst-12tx-4gsfp-wv					
Use of Hard-	24-03-2020	5	In Moxa PT-7528 series	N/A	H-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		070420/1461
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1462
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1463
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code.	N/A	H-MOX-PT-7-070420/1464

CVSS 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
			CVE ID : CVE-2020-6989		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1465
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1466
pt-7528-16mst-8tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1467
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code	N/A	H-MOX-PT-7-070420/1468

CVSS 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
			for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1469
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1470
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1471
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application	N/A	H-MOX-PT-7-070420/1472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-20msc-4tx-4gsfp-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1473
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1474
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1475
Out-of-bounds	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	H-MOX-PT-7-070420/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1477
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1478
pt-7528-8msc-16tx-4gsfp-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can	N/A	H-MOX-PT-7-070420/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1480
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1481
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1482
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web	N/A	H-MOX-PT-7-070420/1483

CVSS 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 without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1484
pt-7528-12mst-12tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1485
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1486
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected	N/A	H-MOX-PT-7-070420/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1488
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1489
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1490
pt-7528-16mst-8tx-4gsfp-wv					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1491
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1492
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1493
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute	N/A	H-MOX-PT-7-070420/1494

CVSS 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
			arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1495
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1496
pt-7528-8mst-16tx-4gsfp-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1497
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	H-MOX-PT-7-070420/1498

CVSS 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
			lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1499
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1500
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1501
Weak Password Requirement	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1502

CVSS 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
s			firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
iologik_2512-wl1-jp					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1503
iologik_2512-wl1-jp-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1504
iologik_2542					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear	N/A	H-MOX-IOLO-070420/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			text. **CVE ID : CVE-2020-7003**		
iologik_2542-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1506
iologik_2542-hspa					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1507
iologik_2542-hspa-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1508
iologik_2542-wl1-eu					
Cleartext	24-03-2020	5	In Moxa ioLogik 2500	N/A	H-MOX-IOLO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Transmission of Sensitive Information			series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**		070420/1509
iologik_2542-wl1-eu-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1510
iologik_2542-wl1-us					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1511
iologik_2542-wl1-us-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is	N/A	H-MOX-IOLO-070420/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**		
iologik_2542-wl1-jp					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1513
iologik_2542-wl1-jp-t					
Cleartext Transmission of Sensitive Information	24-03-2020	5	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text. **CVE ID : CVE-2020-7003**	N/A	H-MOX-IOLO-070420/1514
pt-7528-20mst-4tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1516
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1517
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1518
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization.	N/A	H-MOX-PT-7-070420/1519

CVSS 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
			CVE ID : CVE-2020-6993		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1520
pt-7528-8msc-16tx-4gsfp-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1521
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1522
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow	N/A	H-MOX-PT-7-070420/1523

CVSS 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
			confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1524
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1525
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1526
pt-7528-20mst-4tx-4gsfp-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1528
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1529
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1530

CVSS 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
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1531
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1532
pt-7528-8msc-16tx-4gsfp-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1533
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console.	N/A	H-MOX-PT-7-070420/1534

CVSS 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
			CVE ID : CVE-2020-6985		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1535
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1536
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1537
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password	N/A	H-MOX-PT-7-070420/1538

CVSS 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
			requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-8msc-16tx-4gsfp-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1539
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1540
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1541
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1543
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1544
pt-7528-8mst-16tx-4gsfp-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered.	N/A	H-MOX-PT-7-070420/1545

CVSS 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
			CVE ID : CVE-2020-6983		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1546
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1547
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1548
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without	N/A	H-MOX-PT-7-070420/1549

CVSS 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
			authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1550
eds-510e					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a hard-coded cryptographic key, increasing the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6979**	N/A	H-MOX-EDS--070420/1551
Use of Hard-coded Credentials	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, an attacker may gain access to the system without proper authentication. **CVE ID : CVE-2020-6981**	N/A	H-MOX-EDS--070420/1552
Weak Password Requirements	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, weak password requirements may allow an attacker to gain access using brute force. **CVE ID : CVE-2020-6991**	N/A	H-MOX-EDS--070420/1553
Cleartext Transmissio	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or	N/A	H-MOX-EDS--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Sensitive Information			lower, sensitive information is transmitted over some web applications in cleartext. **CVE ID : CVE-2020-6997**		070420/1554
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-7001**	N/A	H-MOX-EDS--070420/1555
Out-of-bounds Write	24-03-2020	10	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the attacker may execute arbitrary codes or target the device, causing it to go out of service. **CVE ID : CVE-2020-7007**	N/A	H-MOX-EDS--070420/1556
pt-7528-24tx-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1557
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a	N/A	H-MOX-PT-7-070420/1558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1559
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1560
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1561
Weak Password Requirement	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	H-MOX-PT-7-070420/1562

CVSS 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
s			lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		
pt-7528-24tx-hv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1563
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1564
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1565
Out-of-	24-03-2020	7.5	In Moxa PT-7528 series	N/A	H-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		070420/1566
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1567
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1568
pt-7528-24tx-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility	N/A	H-MOX-PT-7-070420/1569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that confidential data can be recovered. **CVE ID : CVE-2020-6983**		
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1570
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1571
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1572
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive	N/A	H-MOX-PT-7-070420/1573

CVSS 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
			information from the web service without authorization. **CVE ID : CVE-2020-6993**		
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1574
pt-7528-24tx-wv-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1575
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1576
Use of a Broken or Risky Cryptographi	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or	N/A	H-MOX-PT-7-070420/1577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Algorithm			lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**		
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1578
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1579
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1580

CVSS 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
pt-7528-24tx-wv-wv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1581
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**	N/A	H-MOX-PT-7-070420/1582
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1583
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service	N/A	H-MOX-PT-7-070420/1584

CVSS 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
			condition or execute arbitrary code. **CVE ID : CVE-2020-6989**		
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1585
Weak Password Requirements	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**	N/A	H-MOX-PT-7-070420/1586
pt-7528-12msc-12tx-4gsfp-hv					
Use of Hard-coded Credentials	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered. **CVE ID : CVE-2020-6983**	N/A	H-MOX-PT-7-070420/1587
Use of Hard-coded Credentials	24-03-2020	10	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series	N/A	H-MOX-PT-7-070420/1588

CVSS 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
			firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console. **CVE ID : CVE-2020-6985**		
Use of a Broken or Risky Cryptographic Algorithm	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed. **CVE ID : CVE-2020-6987**	N/A	H-MOX-PT-7-070420/1589
Out-of-bounds Write	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code. **CVE ID : CVE-2020-6989**	N/A	H-MOX-PT-7-070420/1590
Information Exposure	24-03-2020	5	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization. **CVE ID : CVE-2020-6993**	N/A	H-MOX-PT-7-070420/1591
Weak Password	24-03-2020	7.5	In Moxa PT-7528 series firmware, Version 4.0 or	N/A	H-MOX-PT-7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Requirements			lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access. **CVE ID : CVE-2020-6995**		070420/1592
Rockwellautomation					
micrologix_1400					
Cleartext Storage of Sensitive Information	16-03-2020	2.1	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext. **CVE ID : CVE-2020-6980**	N/A	H-ROC-MICR-070420/1593
Use of a Broken or Risky Cryptographic Algorithm	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic function utilized to protect	N/A	H-ROC-MICR-070420/1594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the password in MicroLogix is discoverable. **CVE ID : CVE-2020-6984**		
Improper Authentication	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials. **CVE ID : CVE-2020-6988**	N/A	H-ROC-MICR-070420/1595
Use of Hard-coded Credentials	16-03-2020	10	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect	N/A	H-ROC-MICR-070420/1596

CVSS 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
			the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller. **CVE ID : CVE-2020-6990**		
micrologix_1100					
Cleartext Storage of Sensitive Information	16-03-2020	2.1	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext. **CVE ID : CVE-2020-6980**	N/A	H-ROC-MICR-070420/1597
Use of a Broken or Risky Cryptographic Algorithm	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and	N/A	H-ROC-MICR-070420/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, The cryptographic function utilized to protect the password in MicroLogix is discoverable. **CVE ID : CVE-2020-6984**		
Improper Authenticati on	16-03-2020	5	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials. **CVE ID : CVE-2020-6988**	N/A	H-ROC-MICR-070420/1599
Use of Hard-coded Credentials	16-03-2020	10	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and	N/A	H-ROC-MICR-070420/1600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, The cryptographic key utilized to help protect the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller. **CVE ID : CVE-2020-6990**		
Samsung					
exynos					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-03-2020	10	An issue was discovered on Samsung mobile devices with any (before February 2020 for Exynos modem chipsets) software. There is a buffer overflow in baseband CP message decoding. The Samsung IDs are SVE-2019-15816 and SVE-2019-15817 (February 2020). **CVE ID : CVE-2020-10835**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-070420/1601
exynos_9610					
Improper Release of Memory Before Removing Last Reference	24-03-2020	3.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 9610 chipsets) software. There is a kernel pointer leak in the vipx driver. The Samsung ID is SVE-2019-	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-070420/1602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16293 (February 2020). **CVE ID : CVE-2020-10840**		
N/A	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 9610 chipsets) software. There is an arbitrary kfree in the vipx and vertex drivers. The Samsung ID is SVE-2019-16294 (February 2020). **CVE ID : CVE-2020-10841**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-070420/1603
galaxy_note8					
Improper Authentication	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) (Galaxy S8 and Note8) software. Facial recognition can be spoofed. The Samsung ID is SVE-2019-16614 (February 2020). **CVE ID : CVE-2020-10847**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-GALA-070420/1604
galaxy_s8					
Improper Authentication	24-03-2020	4.6	An issue was discovered on Samsung mobile devices with P(9.0) (Galaxy S8 and Note8) software. Facial recognition can be spoofed. The Samsung ID is SVE-2019-16614 (February 2020). **CVE ID : CVE-2020-**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-GALA-070420/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10847		
exynos_9810					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-03-2020	10	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos 9810 chipsets) software. Arbitrary memory mapping exists in TEE. The Samsung ID is SVE-2019-16665 (February 2020). **CVE ID : CVE-2020-10848**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-070420/1606
Improper Restriction of Excessive Authentication Attempts	24-03-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos7885, Exynos8895, and Exynos9810 chipsets) software. The Gatekeeper trustlet allows a brute-force attack on the screen lock password. The Samsung ID is SVE-2019-14575 (January 2020). **CVE ID : CVE-2020-10849**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-070420/1607
exynos_7885					
Improper Restriction of Excessive Authentication Attempts	24-03-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos7885, Exynos8895, and Exynos9810 chipsets) software. The Gatekeeper trustlet allows a brute-force attack on the screen lock password. The	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-070420/1608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Samsung ID is SVE-2019-14575 (January 2020). **CVE ID : CVE-2020-10849**		
exynos_8895					
Improper Restriction of Excessive Authentication Attempts	24-03-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos7885, Exynos8895, and Exynos9810 chipsets) software. The Gatekeeper trustlet allows a brute-force attack on the screen lock password. The Samsung ID is SVE-2019-14575 (January 2020). **CVE ID : CVE-2020-10849**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-070420/1609
Schneider-electric					
tsxp57254m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus.	N/A	H-SCH-TSXP-070420/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7477		
tsxp572634m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXP-070420/1611
tsxp57204m_					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command	N/A	H-SCH-TSXP-070420/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over Modbus. **CVE ID : CVE-2020-7477**		
tsxp571634m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXP-070420/1613
tsxp57154m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a	N/A	H-SCH-TSXP-070420/1614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp57104m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXP-070420/1615
140cpu65150					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial	N/A	H-SCH-140C-070420/1616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140cpu65160					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-140C-070420/1617
140cpu65260					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions),	N/A	H-SCH-140C-070420/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140cpu67261					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-140C-070420/1619
140cpu67060					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated	N/A	H-SCH-140C-070420/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140cpu67160					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-140C-070420/1621
140cpu67260					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium	N/A	H-SCH-140C-070420/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140cpu65860					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-140C-070420/1623
140cpu67861					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all	N/A	H-SCH-140C-070420/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140cpu65160s					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-140C-070420/1625
140cpu67160s					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet –	N/A	H-SCH-140C-070420/1626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
140noe77101					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-140N-070420/1627
140noe77111					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated	N/A	H-SCH-140N-070420/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxh5744m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXH-070420/1629
tsxh5724m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum	N/A	H-SCH-TSXH-070420/1630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp576634m_					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXP-070420/1631
tsxp57554m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions	N/A	H-SCH-TSXP-070420/1632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp575634m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXP-070420/1633
tsxp57454m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module	N/A	H-SCH-TSXP-070420/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp574634m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXP-070420/1635
tsxp573634m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet	N/A	H-SCH-TSXP-070420/1636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**		
tsxp57304m					
Improper Check for Unusual or Exceptional Conditions	23-03-2020	5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus. **CVE ID : CVE-2020-7477**	N/A	H-SCH-TSXP-070420/1637
modicon_m340					
Improper Neutralization of Special Elements in	23-03-2020	7.5	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream	N/A	H-SCH-MODI-070420/1638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			Component ('Injection'), reflective DLL, vulnerability exists in EcoStruxure Control Expert (all versions prior to 14.1 Hot Fix), Unity Pro (all versions), Modicon M340 (all versions prior to V3.20), Modicon M580 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller. **CVE ID : CVE-2020-7475**		
modicon_m580					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-03-2020	7.5	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), reflective DLL, vulnerability exists in EcoStruxure Control Expert (all versions prior to 14.1 Hot Fix), Unity Pro (all versions), Modicon M340 (all versions prior to V3.20), Modicon M580 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller. **CVE ID : CVE-2020-7475**	N/A	H-SCH-MODI-070420/1639
andover_continuum_9680					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1641
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1642
andover_continuum_5740					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1644
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1645
andover_continuum_5720					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1647
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1648
andover_continuum_bcx4040					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1650
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1651
andover_continuum_bcx9640					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1653
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1654
andover_continuum_9900					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1656
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1657
andover_continuum_9940					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1659
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1660
andover_continuum_9941					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1662
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1663
andover_continuum_9924					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1665
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1666
andover_continuum_9702					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1668
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1669
andover_continuum_9200					
Improper Control of Generation	23-03-2020	7.5	A CWE-94: Improper Control of Generation of Code ('Code Injection')	N/A	H-SCH-ANDO-070420/1670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data. **CVE ID : CVE-2020-7480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7481**	N/A	H-SCH-ANDO-070420/1671
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-03-2020	4.3	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server. **CVE ID : CVE-2020-7482**	N/A	H-SCH-ANDO-070420/1672
Sonicwall					
sma1000					
Inconsistent Interpretatio	26-03-2020	5	A vulnerability in the SonicWall SMA1000 HTTP	https://psirt.global.sonic	H-SON-SMA1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of HTTP Requests ('HTTP Request Smuggling')			Extraweb server allows an unauthenticated remote attacker to cause HTTP server crash which leads to Denial of Service. This vulnerability affected SMA1000 Version 12.1.0-06411 and earlier. **CVE ID : CVE-2020-5129**	wall.com/vuln-detail/SNWLID-2020-0002	070420/1673
Systech					
nds\/5008rm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	6	Systech Corporation NDS-5000 Terminal Server, NDS/5008 (8 Port, RJ45), firmware Version 02D.30. Successful exploitation of this vulnerability could allow information disclosure, limit system availability, and may allow remote code execution. **CVE ID : CVE-2020-7006**	N/A	H-SYS-NDS\-070420/1674
nds-5000					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-03-2020	6	Systech Corporation NDS-5000 Terminal Server, NDS/5008 (8 Port, RJ45), firmware Version 02D.30. Successful exploitation of this vulnerability could allow information disclosure, limit system availability, and may allow remote code execution. **CVE ID : CVE-2020-7006**	N/A	H-SYS-NDS--070420/1675
zebra					
fx9500					
Improper Limitation of	23-03-2020	5	Motorola FX9500 devices allow remote attackers to	N/A	H-ZEB-FX95-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			conduct absolute path traversal attacks, as demonstrated by PL/SQL Server Pages files such as /include/viewtagdb.psp. **CVE ID : CVE-2020-10875**		070420/1676