National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 31 Aug 2020 Vol. 07 No. 16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
13enforme					
13enforme_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-20	7.5	13enforme CMS 1.0 has SQL Injection via the 'content.php' id parameter. **CVE ID : CVE-2020-23979**	N/A	A-13E-13EN-070920/1
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-20	4.3	13enforme CMS 1.0 has Cross Site Scripting via the "content.php" id parameter. **CVE ID : CVE-2020-23981**	N/A	A-13E-13EN-070920/2
Adobe					
acrobat_dc					
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9721**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/3
Use After	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and	https://helpx.adobe.co	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9722**	m/security/products/acrobat/apsb20-48.html	070920/4
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9723**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/5
Out-of-bounds Write	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9693**	N/A	A-ADO-ACRO-070920/6
Out-of-bounds Write	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9694**	N/A	A-ADO-ACRO-070920/7

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
Incorrect Authorization	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9696**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/8
Information Exposure	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a disclosure of sensitive data vulnerability. Successful exploitation could lead to memory leak. **CVE ID : CVE-2020-9697**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/9
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9698**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/10
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/11

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
			CVE ID : CVE-2020-9699		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9700**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/12
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9701**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/13
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9702**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/14
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability.	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/15

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
			Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9703**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9704**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/16
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9705**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/17
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9706**	N/A	A-ADO-ACRO-070920/18
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and	N/A	A-ADO-ACRO-070920/19

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-2020-9707**		
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9710**	N/A	A-ADO-ACRO-070920/20
Incorrect Authorization	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9712**	N/A	A-ADO-ACRO-070920/21
Improper Privilege Management	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation . **CVE ID : CVE-2020-9714**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/22
Use After Free	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier,	N/A	A-ADO-ACRO-070920/23

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 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9715**		
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9716**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/24
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9717**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/25
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9718**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/26
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002,	https://helpx.adobe.com/security	A-ADO-ACRO-070920/27

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
			2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9719**	/products/acrobat/apsb20-48.html	
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9720**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/28
acrobat_reader_dc					
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9721**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/29
Use After Free	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9722**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/30

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
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9723**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/31
Out-of-bounds Write	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9693**	N/A	A-ADO-ACRO-070920/32
Out-of-bounds Write	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9694**	N/A	A-ADO-ACRO-070920/33
Incorrect Authorization	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9696		
Information Exposure	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a disclosure of sensitive data vulnerability. Successful exploitation could lead to memory leak. **CVE ID : CVE-2020-9697**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/35
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9698**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/36
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9699**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/37
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2020-9700**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9701**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/39
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9702**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/40
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9703**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/41
Buffer Copy without Checking Size of Input ('Classic	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-070920/42

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
Buffer Overflow')			earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9704**	b20-48.html	
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9705**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/43
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9706**	N/A	A-ADO-ACRO-070920/44
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9707**	N/A	A-ADO-ACRO-070920/45
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier,	N/A	A-ADO-ACRO-070920/46

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 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9710**		
Incorrect Authorization	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9712**	N/A	A-ADO-ACRO-070920/47
Improper Privilege Management	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation . **CVE ID : CVE-2020-9714**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/48
Use After Free	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9715**	N/A	A-ADO-ACRO-070920/49
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002,	https://helpx.adobe.com/security	A-ADO-ACRO-070920/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9716**	/products/acrobat/apsb20-48.html	
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9717**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/51
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9718**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/52
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9719**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	A-ADO-ACRO-070920/53
Out-of-	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and	https://helpx.adobe.co	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9720**	m/security/products/acrobat/apsb20-48.html	070920/54
lightroom					
Improper Privilege Management	19-Aug-20	6.8	Adobe Lightroom versions 9.2.0.10 and earlier have an insecure library loading vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9724**	https://helpx.adobe.com/security/products/lightroom/apsb20-51.html	A-ADO-LIGH-070920/55
Apache					
solr					
Improper Input Validation	17-Aug-20	6.5	Reported in SOLR-14515 (private) and fixed in SOLR-14561 (public), released in Solr version 8.6.0. The Replication handler (https://lucene.apache.org/solr/guide/8_6/index-replication.html#http-api-commands-for-the-replicationhandler) allows commands backup, restore and deleteBackup. Each of these take a location parameter, which was not validated, i.e you could read/write to any location the solr user can access. **CVE ID : CVE-2020-13941**	N/A	A-APA-SOLR-070920/56
shiro					
Improper	17-Aug-20	5	Apache Shiro before 1.6.0,	N/A	A-APA-SHIR-

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
Authentication			when using Apache Shiro, a specially crafted HTTP request may cause an authentication bypass. **CVE ID : CVE-2020-13933**		070920/57
auth0					
lock					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-20	3.5	In auth0-lock versions before and including 11.25.1, dangerouslySetInnerHTML is used to update the DOM. When dangerouslySetInnerHTML is used, the application and its users might be exposed to cross-site scripting (XSS) attacks. **CVE ID : CVE-2020-15119**	https://github.com/auth0/lock/security/advisories/GHSA-6gg3-pmm7-97xc	A-AUT-LOCK-070920/58
Cisco					
cyber_vision_center					
Missing Authentication for Critical Function	17-Aug-20	5	A vulnerability in an access control mechanism of Cisco Cyber Vision Center Software could allow an unauthenticated, remote attacker to bypass authentication and access internal services that are running on an affected device. The vulnerability is due to insufficient enforcement of access control in the software. An attacker could exploit this vulnerability by directly accessing the internal services of an affected device. A successful exploit could allow an attacker to impact monitoring of sensors that are	N/A	A-CIS-CYBE-070920/59

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
			managed by the software. **CVE ID : CVE-2020-3448**		
virtualized_packet_core-single_instance					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.8	A vulnerability in the IPv6 implementation of Cisco StarOS could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet to an affected device with the goal of reaching the vulnerable section of the input buffer. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3500**	N/A	A-CIS-VIRT-070920/60
ucs_director					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A vulnerability in the web-based management interface of Cisco UCS Director could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management	N/A	A-CIS-UCS_-070920/61

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
			interface does not properly validate input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need administrative credentials on the affected device. **CVE ID : CVE-2020-3464**		
content_security_management_appliance					
Information Exposure Through Log Files	17-Aug-20	4	A vulnerability in the CLI of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco AsyncOS for Cisco Content Security Management Appliance (SMA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to excessive verbosity in certain log subscriptions. An attacker could exploit this vulnerability by accessing specific log files on an affected device. A successful exploit could allow the attacker to obtain sensitive log data, which may include user credentials. To exploit this vulnerability, the attacker would need to have valid	N/A	A-CIS-CONT-070920/62

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
			credentials at the operator level or higher on the affected device. **CVE ID : CVE-2020-3447**		
anyconnect_secure_mobility_client					
Uncontrolled Search Path Element	17-Aug-20	7.2	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. **CVE ID : CVE-2020-3433**	N/A	A-CIS-ANYC-070920/63
Improper Input Validation	17-Aug-20	4.9	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local	N/A	A-CIS-ANYC-070920/64

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
			attacker to cause a denial of service (DoS) condition on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process on an affected device. A successful exploit could allow the attacker to stop the AnyConnect process, causing a DoS condition on the device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. **CVE ID : CVE-2020-3434**		
Improper Input Validation	17-Aug-20	2.1	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to overwrite VPN profiles on an affected device. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted IPC message to the	N/A	A-CIS-ANYC-070920/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AnyConnect process on an affected device. A successful exploit could allow the attacker to modify VPN profile files. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. **CVE ID : CVE-2020-3435**		
data_center_network_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	3.5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3439**	N/A	A-CIS-DATA-070920/66
Improper Neutralization of Input During Web Page Generation	26-Aug-20	3.5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a	N/A	A-CIS-DATA-070920/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			cross-site scripting (XSS) attack against a user of the interface of the affected software. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3518**		
Improper Input Validation	26-Aug-20	5.5	A vulnerability in a specific REST API method of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a path traversal attack on an affected device. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2020-3519**	N/A	A-CIS-DATA-070920/68
Information Exposure	26-Aug-20	2.1	A vulnerability in Cisco Data Center Network Manager	N/A	A-CIS-DATA-070920/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DCNM) Software could allow an authenticated, local attacker to obtain confidential information from an affected device. The vulnerability is due to insufficient protection of confidential information on an affected device. An attacker at any privilege level could exploit this vulnerability by accessing local filesystems and extracting sensitive information from them. A successful exploit could allow the attacker to view sensitive data, which they could use to elevate their privilege. **CVE ID : CVE-2020-3520**		
Improper Input Validation	26-Aug-20	4	A vulnerability in a specific REST API of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker with a low-privileged account could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to read arbitrary files on the affected system. **CVE ID : CVE-2020-3521**	N/A	A-CIS-DATA-070920/70
dna_center					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-Aug-20	5	A vulnerability in Cisco DNA Center software could allow an unauthenticated remote attacker access to sensitive information on an affected system. The vulnerability is due to improper handling of authentication tokens by the affected software. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker access to sensitive device information, which includes configuration files. **CVE ID : CVE-2020-3411**	N/A	A-CIS-DNA_-070920/71
email_security_appliance					
Information Exposure Through Log Files	17-Aug-20	4	A vulnerability in the CLI of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco AsyncOS for Cisco Content Security Management Appliance (SMA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to excessive verbosity in certain log subscriptions. An attacker could exploit this vulnerability by accessing specific log files on an affected device. A successful exploit could allow the attacker to obtain sensitive log data, which may include user credentials. To exploit this vulnerability, the attacker	N/A	A-CIS-EMAI-070920/72

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid credentials at the operator level or higher on the affected device. **CVE ID : CVE-2020-3447**		
unified_communications_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	4.3	A vulnerability in the web UI of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web UI does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2020-3346**	N/A	A-CIS-UNIF-070920/73
webex_meetings_online					
Incorrect Authorization	17-Aug-20	4	A vulnerability in the scheduled meeting template feature of Cisco Webex Meetings could allow an authenticated, remote	N/A	A-CIS-WEBE-070920/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to create a scheduled meeting template that would belong to another user in their organization. The vulnerability is due to insufficient authorization enforcement for the creation of scheduled meeting templates. An attacker could exploit this vulnerability by sending a crafted request to the Webex Meetings interface to create a scheduled meeting template. A successful exploit could allow the attacker to create a scheduled meeting template that would belong to a user other than themselves. **CVE ID : CVE-2020-3412**		
Incorrect Authorization	17-Aug-20	4	A vulnerability in the scheduled meeting template feature of Cisco Webex Meetings could allow an authenticated, remote attacker to delete a scheduled meeting template that belongs to another user in their organization. The vulnerability is due to insufficient authorization enforcement for requests to delete scheduled meeting templates. An attacker could exploit this vulnerability by sending a crafted request to the Webex Meetings interface to delete a scheduled meeting template. A successful exploit could allow the attacker to delete a scheduled meeting template that belongs to a	N/A	A-CIS-WEBE-070920/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user other than themselves. **CVE ID : CVE-2020-3413**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	4.3	A vulnerability in the web-based management interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected service. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected service. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3463**	N/A	A-CIS-WEBE-070920/76
Information Exposure	17-Aug-20	4	A vulnerability in the contacts feature of Cisco Webex Meetings could allow an authenticated, remote attacker with a legitimate user account to access sensitive information. The vulnerability is due to improper access restrictions on users who are added within user contacts. An attacker on one Webex Meetings site could exploit	N/A	A-CIS-WEBE-070920/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending specially crafted requests to the Webex Meetings site. A successful exploit could allow the attacker to view the details of users on another Webex site, including user names and email addresses. **CVE ID : CVE-2020-3472**		
webex_meetings_server					
Improper Input Validation	17-Aug-20	3.5	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users. **CVE ID : CVE-2020-3501**	N/A	A-CIS-WEBE-070920/78
Improper Input Validation	17-Aug-20	3.5	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These	N/A	A-CIS-WEBE-070920/79

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
			vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users. **CVE ID : CVE-2020-3502**		
webex_meetings					
Improper Input Validation	17-Aug-20	3.5	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users. **CVE ID : CVE-2020-3501**	N/A	A-CIS-WEBE-070920/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Aug-20	3.5	Multiple vulnerabilities in the user interface of Cisco Webex Meetings Desktop App could allow an authenticated, remote attacker to obtain restricted information from other Webex users. These vulnerabilities are due to improper input validation of parameters returned to the application from a web site. An attacker with a valid Webex account could exploit these vulnerabilities by persuading a user to follow a URL that is designed to return malicious path parameters to the affected software. A successful exploit could allow the attacker to obtain restricted information from other Webex users. **CVE ID : CVE-2020-3502**	N/A	A-CIS-WEBE-070920/81
Citrix					
xenmobile_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	4.3	Improper input validation in Citrix XenMobile Server 10.12 before RP1, Citrix XenMobile Server 10.11 before RP4, Citrix XenMobile Server 10.11 before RP6 and Citrix XenMobile Server before 10.9 RP5 allows Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8208**	N/A	A-CIT-XENM-070920/82
Improper Limitation of a Pathname to a	17-Aug-20	5	Improper access control in Citrix XenMobile Server 10.12 before RP2, Citrix XenMobile Server 10.11 before RP4,	N/A	A-CIT-XENM-070920/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			Citrix XenMobile Server 10.10 before RP6 and Citrix XenMobile Server before 10.9 RP5 and leads to the ability to read arbitrary files. **CVE ID : CVE-2020-8209**		
Insufficiently Protected Credentials	17-Aug-20	5	Insufficient protection of secrets in Citrix XenMobile Server 10.12 before RP3, Citrix XenMobile Server 10.11 before RP6, Citrix XenMobile Server 10.10 RP6 and Citrix XenMobile Server before 10.9 RP5 discloses credentials of a service account. **CVE ID : CVE-2020-8210**	N/A	A-CIT-XENM-070920/84
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Aug-20	7.5	Improper input validation in Citrix XenMobile Server 10.12 before RP3, Citrix XenMobile Server 10.11 before RP6, Citrix XenMobile Server 10.10 RP6 and Citrix XenMobile Server before 10.9 RP5 allows SQL Injection. **CVE ID : CVE-2020-8211**	N/A	A-CIT-XENM-070920/85
Incorrect Authorization	17-Aug-20	7.5	Improper access control in Citrix XenMobile Server 10.12 before RP3, Citrix XenMobile Server 10.11 before RP6, Citrix XenMobile Server 10.10 RP6 and Citrix XenMobile Server before 10.9 RP5 allows access to privileged functionality. **CVE ID : CVE-2020-8212**	N/A	A-CIT-XENM-070920/86
cloudfoundry					
cf-deployment					
Improper	21-Aug-20	4	Cloud Foundry Routing	https://ww	A-CLO-CF-D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Shutdown or Release			(Gorouter), versions prior to 0.204.0, when used in a deployment with NGINX reverse proxies in front of the Gorouters, is potentially vulnerable to denial-of-service attacks in which an unauthenticated malicious attacker can send specially-crafted HTTP requests that may cause the Gorouters to be dropped from the NGINX backend pool. **CVE ID : CVE-2020-5416**	w.cloudfoundry.org/blog/cve-2020-5416	070920/87
Incorrect Permission Assignment for Critical Resource	21-Aug-20	6.5	Cloud Foundry CAPI (Cloud Controller), versions prior to 1.97.0, when used in a deployment where an app domain is also the system domain (which is true in the default CF Deployment manifest), were vulnerable to developers maliciously or accidentally claiming certain sensitive routes, potentially resulting in the developer's app handling some requests that were expected to go to certain system components. **CVE ID : CVE-2020-5417**	https://www.cloudfoundry.org/blog/cve-2020-5417	A-CLO-CF-D-070920/88
cloud_controller					
Incorrect Permission Assignment for Critical Resource	21-Aug-20	6.5	Cloud Foundry CAPI (Cloud Controller), versions prior to 1.97.0, when used in a deployment where an app domain is also the system domain (which is true in the default CF Deployment manifest), were vulnerable to developers maliciously or	https://www.cloudfoundry.org/blog/cve-2020-5417	A-CLO-CLOU-070920/89

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
			accidentally claiming certain sensitive routes, potentially resulting in the developer's app handling some requests that were expected to go to certain system components. **CVE ID : CVE-2020-5417**		
routing					
Improper Resource Shutdown or Release	21-Aug-20	4	Cloud Foundry Routing (Gorouter), versions prior to 0.204.0, when used in a deployment with NGINX reverse proxies in front of the Gorouters, is potentially vulnerable to denial-of-service attacks in which an unauthenticated malicious attacker can send specially-crafted HTTP requests that may cause the Gorouters to be dropped from the NGINX backend pool. **CVE ID : CVE-2020-5416**	https://www.cloudfoundry.org/blog/cve-2020-5416	A-CLO-ROUT-070920/90
Codiad					
codiad					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-20	4.3	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** A Cross Site Scripting (XSS) vulnerability was found in Codiad v1.7.8 and later. The vulnerability occurs because of improper sanitization of the folder's name $path variable in components/filemanager/class.filemanager.php. NOTE: the vendor states "Codiad is no longer under active maintenance by core	N/A	A-COD-CODI-070920/91

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
			contributors." **CVE ID : CVE-2020-14042**		
cogboard					
red_discord_bot					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Aug-20	5.5	In Red Discord Bot before version 3.3.11, a RCE exploit has been discovered in the Trivia module: this exploit allows Discord users with specifically crafted usernames to inject code into the Trivia module's leaderboard command. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. This critical exploit has been fixed on version 3.3.11. **CVE ID : CVE-2020-15140**	https://github.com/Cog-Creators/Red-DiscordBot/security/advisories/GHSA-55j9-849x-26h4	A-COG-RED_-070920/92
Improper Control of Generation of Code ('Code Injection')	21-Aug-20	6	Red Discord Bot before versions 3.3.12 and 3.4 has a Remote Code Execution vulnerability in the Streams module. This exploit allows Discord users with specifically crafted "going live" messages to inject code into the Streams module's going live message. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. As a workaround, unloading the Trivia module with `unload streams` can render this exploit not accessible. It is highly recommended updating to 3.3.12 or 3.4 to	https://github.com/Cog-Creators/Red-DiscordBot/security/advisories/GHSA-7257-96vg-qf6x	A-COG-RED_-070920/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			completely patch this issue. **CVE ID : CVE-2020-15147**		
connie-lang_project					
connie-lang					
Improper Input Validation	18-Aug-20	7.5	The package connie-lang before 0.1.1 are vulnerable to Prototype Pollution in the configuration language library used by connie. **CVE ID : CVE-2020-7706**	N/A	A-CON-CONN-070920/94
cookielawinfo					
gdpr_cookie_consent					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-20	3.5	ajax_policy_generator in admin/modules/cli-policy-generator/classes/class-policy-generator-ajax.php in GDPR Cookie Consent (cookie-law-info) 1.8.2 and below plugin for WordPress, allows authenticated stored XSS and privilege escalation. **CVE ID : CVE-2020-20633**	N/A	A-COO-GDPR-070920/95
cybersolutions					
cybermail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-20	4.3	Cross-site scripting vulnerability in CyberMail Ver.6.x and Ver.7.x allows remote attackers to inject arbitrary script or HTML via a specially crafted URL. **CVE ID : CVE-2020-5540**	N/A	A-CYB-CYBE-070920/96
URL Redirection to Untrusted Site ('Open Redirect')	25-Aug-20	5.8	Open redirect vulnerability in CyberMail Ver.6.x and Ver.7.x allows remote attackers to redirect users to arbitrary sites and conduct phishing	N/A	A-CYB-CYBE-070920/97

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
			attacks via a specially crafted URL. **CVE ID : CVE-2020-5541**		
dbhcms_project					
dbhcms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Aug-20	5	DBHcms v1.2.0 has a directory traversal vulnerability as there is no directory control function in directory /dbhcms/. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information. **CVE ID : CVE-2020-19877**	N/A	A-DBH-DBHC-070920/98
Information Exposure	24-Aug-20	5	DBHcms v1.2.0 has a sensitive information leaks vulnerability as there is no security access control in /dbhcms/ext/news/ext.news.be.php, A remote unauthenticated attacker can exploit this vulnerability to get path information. **CVE ID : CVE-2020-19878**	N/A	A-DBH-DBHC-070920/99
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-20	4.3	DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter of $_GET['dbhcms_pid'] variable in dbhcms\page.php line 107, **CVE ID : CVE-2020-19879**	N/A	A-DBH-DBHC-070920/100
Improper Neutralization of Input During Web Page	24-Aug-20	4.3	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function form 'Name' in dbhcms\types.php, A remote	N/A	A-DBH-DBHC-070920/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			unauthenticated attacker can exploit this vulnerability to hijack other users. **CVE ID : CVE-2020-19880**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-20	3.5	DBHcms v1.2.0 has a reflected xss vulnerability as there is no security filter in dbhcms\mod\mod.selector.php line 108 for $_GET['return_name'] parameter, A remote authenticated with admin user can exploit this vulnerability to hijack other users. **CVE ID : CVE-2020-19881**	N/A	A-DBH-DBHC-070920/102
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-20	3.5	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for 'menu_description' variable in dbhcms\mod\mod.menus.edit.php line 83 and in dbhcms\mod\mod.menus.view.php line 111, A remote authenticated with admin user can exploit this vulnerability to hijack other users. **CVE ID : CVE-2020-19882**	N/A	A-DBH-DBHC-070920/103
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-20	3.5	DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter in dbhcms\mod\mod.users.view.php line 57 for user_login, A remote authenticated with admin user can exploit this vulnerability to hijack other users. **CVE ID : CVE-2020-19883**	N/A	A-DBH-DBHC-070920/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-20	3.5	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function in dbhcms\mod\mod.domain.edit.php line 119. **CVE ID : CVE-2020-19884**	N/A	A-DBH-DBHC-070920/105
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-20	3.5	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_name']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users. **CVE ID : CVE-2020-19885**	N/A	A-DBH-DBHC-070920/106
Cross-Site Request Forgery (CSRF)	24-Aug-20	4.3	DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for an /index.php?dbhcms_pid=-80&deletemenu=9 can delete any menu. **CVE ID : CVE-2020-19886**	N/A	A-DBH-DBHC-070920/107
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-20	3.5	DBHcms v1.2.0 has a stored XSS vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_description']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	N/A	A-DBH-DBHC-070920/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-19887		
Incorrect Authorization	24-Aug-20	4.3	DBHcms v1.2.0 has an unauthorized operation vulnerability because there's no access control at line 175 of dbhcms\page.php for empty cache operation. This vulnerability can be exploited to empty a table. **CVE ID : CVE-2020-19888**	N/A	A-DBH-DBHC-070920/109
Cross-Site Request Forgery (CSRF)	24-Aug-20	6.8	DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for index.php?dbhcms_pid=-70 can add a user. **CVE ID : CVE-2020-19889**	N/A	A-DBH-DBHC-070920/110
Information Exposure	24-Aug-20	4	DBHcms v1.2.0 has an Arbitrary file read vulnerability in dbhcms\mod\mod.editor.php $_GET['file'] is filename,and as there is no filter function for security, you can read any file's content. **CVE ID : CVE-2020-19890**	N/A	A-DBH-DBHC-070920/111
Out-of-bounds Write	24-Aug-20	6.5	DBHcms v1.2.0 has an Arbitrary file write vulnerability in dbhcms\mod\mod.editor.php $_POST['updatefile'] is filename and $_POST['tinymce_content'] is file content, there is no filter function for security. A remote authenticated admin user can exploit this vulnerability to get a webshell.	N/A	A-DBH-DBHC-070920/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-19891		
dbsoft					
sglac					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Aug-20	7.5	An issue was discovered in DB Soft SGLAC before 20.05.001. The ProcedimientoGenerico method in the SVCManejador.svc webservice of the SGLAC web frontend allows an attacker to run arbitrary SQL commands on the SQL Server. Command execution can be easily achieved by using the xp_cmdshell stored procedure. **CVE ID : CVE-2020-12606**	N/A	A-DBS-SGLA-070920/113
Dell					
encryption					
Incorrect Permission Assignment for Critical Resource	18-Aug-20	7.2	Dell Encryption versions prior to 10.8 and Dell Endpoint Security Suite versions prior to 2.8 contain a privilege escalation vulnerability because of an incomplete fix for CVE-2020-5358. A local malicious user with low privileges could potentially exploit this vulnerability to gain elevated privilege on the affected system with the help of a symbolic link. **CVE ID : CVE-2020-5385**	N/A	A-DEL-ENCR-070920/114
endpoint_security_suite_enterprise					
Incorrect Permission Assignment for Critical	18-Aug-20	7.2	Dell Encryption versions prior to 10.8 and Dell Endpoint Security Suite versions prior to 2.8 contain a privilege	N/A	A-DEL-ENDP-070920/115

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
Resource			escalation vulnerability because of an incomplete fix for CVE-2020-5358. A local malicious user with low privileges could potentially exploit this vulnerability to gain elevated privilege on the affected system with the help of a symbolic link. **CVE ID : CVE-2020-5385**		
dieboldnixdorf					
probase					
Missing Encryption of Sensitive Data	21-Aug-20	2.1	Diebold Nixdorf ProCash 2100xe USB ATMs running Wincor Probase version 1.1.30 do not encrypt, authenticate, or verify the integrity of messages between the CCDM and the host computer, allowing an attacker with physical access to internal ATM components to commit deposit forgery by intercepting and modifying messages to the host computer, such as the amount and value of currency being deposited. **CVE ID : CVE-2020-9062**	N/A	A-DIE-PROB-070920/116
Dolibarr					
dolibarr					
Improper Privilege Management	21-Aug-20	4	Dolibarr CRM before 11.0.5 allows privilege escalation. This could allow remote authenticated attackers to upload arbitrary files via societe/document.php in which "disabled" is changed to "enabled" in the HTML	https://github.com/Dolibarr/dolibarr/blob/develop/ChangeLog	A-DOL-DOLI-070920/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			source code. **CVE ID : CVE-2020-14201**		
dronecode					
micro_air_vehicle_link					
Improper Authentication	20-Aug-20	7.5	The Micro Air Vehicle Link (MAVLink) protocol presents authentication mechanisms on its version 2.0 however according to its documentation, in order to maintain backwards compatibility, GCS and autopilot negotiate the version via the AUTOPILOT_VERSION message. Since this negotiation depends on the answer, an attacker may craft packages in a way that hints the autopilot to adopt version 1.0 of MAVLink for the communication. Given the lack of authentication capabilities in such version of MAVLink (refer to CVE-2020-10282), attackers may use this method to bypass authentication capabilities and interact with the autopilot directly. **CVE ID : CVE-2020-10283**	https://github.com/aliasrobotics/RVD/issues/3316	A-DRO-MICR-070920/118
Elastic					
enterprise_search					
Improper Privilege Management	18-Aug-20	4	Elastic Enterprise Search before 7.9.0 contain a credential exposure flaw in the App Search interface. If a user is given the ï¿½developerï¿½ role, they	N/A	A-ELA-ENTE-070920/119

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
			will be able to view the administrator API credentials. These credentials could allow the developer user to conduct operations with the same permissions of the App Search administrator. **CVE ID : CVE-2020-7018**		
elasticsearch					
Improper Privilege Management	18-Aug-20	4	In Elasticsearch before 7.9.0 and 6.8.12 a field disclosure flaw was found when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden. This could result in an attacker gaining additional permissions against a restricted index. **CVE ID : CVE-2020-7019**	https://security.netapp.com/advisory/ntap-20200827-0001/	A-ELA-ELAS-070920/120
elementor					
elementor_page_builder					
Incorrect Permission Assignment for Critical Resource	21-Aug-20	4	Elementor 2.9.5 and below WordPress plugin allows authenticated users to activate its safe mode feature. This can be exploited to disable all security plugins on the blog. **CVE ID : CVE-2020-20634**	N/A	A-ELE-ELEM-070920/121
emclient					
em_client					
Improper Certificate	20-Aug-20	5.8	eM Client before 7.2.33412.0 automatically imported S/MIME certificates and	N/A	A-EMC-EM_C-070920/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			thereby silently replaced existing ones. This allowed a man-in-the-middle attacker to obtain an email-validated S/MIME certificate from a trusted CA and replace the public key of the entity to be impersonated. This enabled the attacker to decipher further communication. The entire attack could be accomplished by sending a single email. **CVE ID : CVE-2020-12618**		
exceedone					
exment					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-20	3.5	Cross-site scripting vulnerability in Exment prior to v3.6.0 allows remote authenticated attackers to inject arbitrary script or HTML via unspecified vectors. **CVE ID : CVE-2020-5619**	N/A	A-EXC-EXME-070920/123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-20	3.5	Cross-site scripting vulnerability in Exment prior to v3.6.0 allows remote authenticated attackers to inject arbitrary script or HTML via a specially crafted file. **CVE ID : CVE-2020-5620**	N/A	A-EXC-EXME-070920/124
Foxitsoftware					
foxit_studio_photo					
Out-of-bounds Write	20-Aug-20	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio	N/A	A-FOX-FOXI-070920/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Photo 3.6.6.922. 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 TIF 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 context of the current process. Was ZDI-CAN-10764. **CVE ID : CVE-2020-15629**		
Out-of-bounds Read	20-Aug-20	6.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. 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 PNG 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-	N/A	A-FOX-FOXI-070920/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-10977. **CVE ID : CVE-2020-15630**		
Stack-based Buffer Overflow	20-Aug-20	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 TIF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9881. **CVE ID : CVE-2020-8869**	N/A	A-FOX-FOXI-070920/127
Out-of-bounds Read	20-Aug-20	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 TIF files from the GetTIFPalette method. The issue results from the lack of proper validation of user-supplied data, which can	N/A	A-FOX-FOXI-070920/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-9931. **CVE ID : CVE-2020-8870**		
phantompdf					
Use After Free	20-Aug-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. 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 SetLocalDescription method. By performing actions in JavaScript, an attacker can cause a pointer to be reused after it has been freed. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10972. **CVE ID : CVE-2020-15637**	N/A	A-FOX-PHAN-070920/129
Access of Resource Using Incompatible Type ('Type Confusion')	20-Aug-20	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.2.29539. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a	N/A	A-FOX-PHAN-070920/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. The specific flaw exists within the NodeProperties::InferReceiverMapsUnsafe method. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10950. **CVE ID : CVE-2020-15638**		
reader					
Use After Free	20-Aug-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. 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 SetLocalDescription method. By performing actions in JavaScript, an attacker can cause a pointer to be reused after it has been freed. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10972. **CVE ID : CVE-2020-15637**	N/A	A-FOX-READ-070920/131
Access of Resource	20-Aug-20	6.8	This vulnerability allows remote attackers to execute	N/A	A-FOX-READ-

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
Using Incompatible Type ('Type Confusion')			arbitrary code on affected installations of Foxit PhantomPDF 9.7.2.29539. 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 NodeProperties::InferReceiverMapsUnsafe method. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10950. **CVE ID : CVE-2020-15638**		070920/132
freron					
mailmate					
Improper Certificate Validation	20-Aug-20	4.3	MailMate before 1.11 automatically imported S/MIME certificates and thereby silently replaced existing ones. This allowed a man-in-the-middle attacker to obtain an email-validated S/MIME certificate from a trusted CA and replace the public key of the entity to be impersonated. This enabled the attacker to decipher further communication. The entire attack could be accomplished by sending a single email.	N/A	A-FRE-MAIL-070920/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12619		
ftp-srv_project					
ftp-srv					
Server-Side Request Forgery (SSRF)	17-Aug-20	5	ftp-srv versions 1.0.0 through 4.3.3 are vulnerable to Server-Side Request Forgery. The PORT command allows arbitrary IPs which can be used to cause the server to make a connection elsewhere. A possible workaround is blocking the PORT through the configuration. This issue is fixed in version 4.3.4. More information can be found on the linked advisory. **CVE ID : CVE-2020-15152**	https://github.com/autovance/ftp-srv/security/advisories/GHSA-jw37-5gqr-cf9j	A-FTP-FTP--070920/134
gog					
galaxy					
Improper Privilege Management	21-Aug-20	6.9	The client (aka GalaxyClientService.exe) in GOG GALAXY through 2.0.20 allows local privilege escalation from any authenticated user to SYSTEM by instructing the Windows service to execute arbitrary commands. This occurs because the attacker can inject a DLL into GalaxyClient.exe, defeating the TCP-based "trusted client" protection mechanism. **CVE ID : CVE-2020-24574**	N/A	A-GOG-GALA-070920/135
goxmldsig_project					
goxmldsig					
NULL Pointer	23-Aug-20	5	This affects all versions of package	N/A	A-GOX-GOXM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			github.com/russellhaering/goxmldsig. There is a crash on nil-pointer dereference caused by sending malformed XML signatures. **CVE ID : CVE-2020-7711**		070920/136
gunet					
open_eclass_platform					
Information Exposure	19-Aug-20	4.3	** DISPUTED ** GUnet Open eClass Platform (aka openeclass) through 3.9.2 might allow remote attackers to read students' submitted assessments because it does not ensure that the web server blocks directory listings. NOTE: this is disputed because it only affects misconfigured installations. **CVE ID : CVE-2020-24381**	https://github.com/gunet/openeclass/issues/39	A-GUN-OPEN-070920/137
hashicorp					
vault-ssh-helper					
Improper Input Validation	20-Aug-20	5	HashiCorp vault-ssh-helper up to and including version 0.1.6 incorrectly accepted Vault-issued SSH OTPs for the subnet in which a host's network interface was located, rather than the specific IP address assigned to that interface. Fixed in 0.2.0. **CVE ID : CVE-2020-24359**	N/A	A-HAS-VAUL-070920/138
Huawei					
fusioncompute					
Improper Authenticatio	17-Aug-20	6.4	FusionCompute 8.0.0 have an insufficient authentication	N/A	A-HUA-FUSI-070920/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			vulnerability. An attacker may exploit the vulnerability to delete some files and cause some services abnormal. **CVE ID : CVE-2020-9233**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	6.5	FusionCompute 8.0.0 have a command injection vulnerability. The software does not sufficiently validate certain parameters post from user, successful exploit could allow an authenticated attacker to launch a command injection attack. **CVE ID : CVE-2020-9242**	N/A	A-HUA-FUSI-070920/140
Information Exposure	21-Aug-20	4	FusionCompute 8.0.0 has an information leak vulnerability. A module does not launch strict access control and information protection. Attackers with low privilege can get some extra information. This can lead to information leak. **CVE ID : CVE-2020-9246**	N/A	A-HUA-FUSI-070920/141
IBM					
planning_analytics					
Incorrect Authorization	19-Aug-20	4	A vulnerability exsists in IBM Planning Analytics 2.0 whereby avatars in Planning Analytics Workspace could be modified by other users without authorization to do so. IBM X-Force ID: 186019. **CVE ID : CVE-2020-4648**	https://www.ibm.com/support/pages/node/6254788	A-IBM-PLAN-070920/142
URL Redirection to Untrusted	19-Aug-20	5.8	IBM Planning Analytics 2.0 could allow a remote attacker to conduct phishing attacks,	https://www.ibm.com/support/pa	A-IBM-PLAN-070920/143

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
Site ('Open Redirect')			using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. **CVE ID : CVE-2020-4653**	ges/node/6254788	
elastic_storage_server					
N/A	19-Aug-20	3.5	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.6 could allow an authenticated user to cause a denial of service during deployment or upgrade if GUI specific services are enabled. IBM X-Force ID: 179162. **CVE ID : CVE-2020-4381**	https://www.ibm.com/support/pages/node/6261435	A-IBM-ELAS-070920/144
Improper Input Validation	24-Aug-20	2.1	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment or upgrade pertaining to xcat services. IBM X-Force ID: 179163. **CVE ID : CVE-2020-4382**	https://www.ibm.com/support/pages/node/6320001	A-IBM-ELAS-070920/145
Improper Input Validation	24-Aug-20	4	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment while configuring	https://www.ibm.com/support/pages/node/6320003	A-IBM-ELAS-070920/146

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
			some of the network services. IBM X-Force ID: 179165. **CVE ID : CVE-2020-4383**		
connect\					
Out-of-bounds Write	24-Aug-20	7.2	IBM Sterling Connect:Direct for UNIX 4.2.0, 4.3.0, 6.0.0, and 6.1.0 is vulnerable to a stack based buffer ovreflow, caused by improper bounds checking. A local attacker could manipulate CD UNIX to obtain root provileges. IBM X-Force ID: 184578. **CVE ID : CVE-2020-4587**	https://www.ibm.com/support/pages/node/6320317	A-IBM-CONN-070920/147
sterling_connect\					
Out-of-bounds Write	24-Aug-20	7.2	IBM Sterling Connect:Direct for UNIX 4.2.0, 4.3.0, 6.0.0, and 6.1.0 is vulnerable to a stack based buffer ovreflow, caused by improper bounds checking. A local attacker could manipulate CD UNIX to obtain root provileges. IBM X-Force ID: 184578. **CVE ID : CVE-2020-4587**	https://www.ibm.com/support/pages/node/6320317	A-IBM-STER-070920/148
spectrum_virtualize					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	A-IBM-SPEC-070920/149
websphere_application_server					
Improper Neutralizatio	27-Aug-20	4.3	IBM WebSphere Application Server ND 8.5 and 9.0, and	https://www.ibm.com/	A-IBM-WEBS-070920/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			IBM WebSphere Virtual Enterprise 7.0 and 8.0 are vulnerable to cross-site scripting when High Availability Deployment Manager is configured. **CVE ID : CVE-2020-4575**	support/pages/node/6323293	
websphere_virtual_enterprise					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-20	4.3	IBM WebSphere Application Server ND 8.5 and 9.0, and IBM WebSphere Virtual Enterprise 7.0 and 8.0 are vulnerable to cross-site scripting when High Availability Deployment Manager is configured. **CVE ID : CVE-2020-4575**	https://www.ibm.com/support/pages/node/6323293	A-IBM-WEBS-070920/151
content_navigator					
Improper Input Validation	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 is vulnerable to improper input validation. A malicious administrator could bypass the user interface and send requests to the IBM Content Navigator server with illegal characters that could be stored in the IBM Content Navigator database. IBM X-Force ID: 183316. **CVE ID : CVE-2020-4548**	https://www.ibm.com/support/pages/node/6262411	A-IBM-CONT-070920/152
Information Exposure	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 could allow an authenticated user to view cached content of another user that they should not have access to. IBM X-Force ID: 186679. **CVE ID : CVE-2020-4687**	https://www.ibm.com/support/pages/node/6262423	A-IBM-CONT-070920/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
security_guardium_insights					
Information Exposure Through an Error Message	27-Aug-20	5	IBM Security Guardium Insights 2.0.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 174402. **CVE ID : CVE-2020-4166**	https://www.ibm.com/support/pages/node/6323297	A-IBM-SECU-070920/154
Improper Authentication	27-Aug-20	6.4	IBM Security Guardium Insights 2.0.1 could allow an attacker to obtain sensitive information or perform unauthorized actions due to improper authenciation mechanisms. IBM X-Force ID: 174403. **CVE ID : CVE-2020-4167**	https://www.ibm.com/support/pages/node/6323297	A-IBM-SECU-070920/155
Use of a Broken or Risky Cryptographic Algorithm	27-Aug-20	5	IBM Security Guardium Insights 2.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174405. **CVE ID : CVE-2020-4169**	https://www.ibm.com/support/pages/node/6323297	A-IBM-SECU-070920/156
Cross-Site Request Forgery (CSRF)	24-Aug-20	4.3	IBM Security Guardium Insights 2.0.1 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: 174406.	https://www.ibm.com/support/pages/node/6320055	A-IBM-SECU-070920/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4170		
Information Exposure	27-Aug-20	4	IBM Security Guardium Insights 2.0.1 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 174407. **CVE ID : CVE-2020-4171**	https://www.ibm.com/support/pages/node/6323297	A-IBM-SECU-070920/158
Insecure Storage of Sensitive Information	27-Aug-20	5	IBM Security Guardium Insights 2.0.1 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 174408. **CVE ID : CVE-2020-4172**	https://www.ibm.com/support/pages/node/6323297	A-IBM-SECU-070920/159
Use of a Broken or Risky Cryptographic Algorithm	27-Aug-20	5	IBM Security Guardium Insights 2.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174683. **CVE ID : CVE-2020-4174**	https://www.ibm.com/support/pages/node/6323297	A-IBM-SECU-070920/160
Insufficiently Protected Credentials	24-Aug-20	2.1	IBM Security Guardium Insights 2.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 184747. **CVE ID : CVE-2020-4593**	https://www.ibm.com/support/pages/node/6320067	A-IBM-SECU-070920/161
URL Redirection to Untrusted Site ('Open	24-Aug-20	5.8	IBM Security Guardium Insights 2.0.1 could allow a remote attacker to conduct phishing attacks, using an	https://www.ibm.com/support/pages/node/6	A-IBM-SECU-070920/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 184823. **CVE ID : CVE-2020-4598**	320061	
Improper Privilege Management	27-Aug-20	6.5	IBM Security Guardium Insights 2.0.1 performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 184880. **CVE ID : CVE-2020-4603**	https://www.ibm.com/support/pages/node/6323297	A-IBM-SECU-070920/163
Icinga					
icinga_web2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Aug-20	4.3	Icinga Icinga Web2 2.0.0 through 2.6.4, 2.7.4 and 2.8.2 has a Directory Traversal vulnerability which allows an attacker to access arbitrary files that are readable by the process running Icinga Web 2. This issue is fixed in Icinga Web 2 in v2.6.4, v2.7.4 and v2.8.2. **CVE ID : CVE-2020-24368**	https://icinga.com/2020/08/19/icinga-web-security-release-v2-6-4-v2-7-4-and-v2-8-2/	A-ICI-ICIN-070920/164

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
I-doit					
i-doit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-20	4.3	A cross-site scripting (XSS) vulnerability in i-doit 1.14.2 allows remote attackers to inject arbitrary web script or HTML via the viewMode, tvMode, tvType, objID, catgID, objTypeID, or editMode parameter. **CVE ID : CVE-2020-13825**	N/A	A-I-D-I-DO-070920/165
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Aug-20	6.8	A CSV injection (aka Excel Macro Injection or Formula Injection) issue in i-doit 1.14.2 allows an attacker to execute arbitrary commands via a Title parameter that is mishandled in a CSV export. **CVE ID : CVE-2020-13826**	N/A	A-I-D-I-DO-070920/166
instructure					
canvas_learning_management_service					
Server-Side Request Forgery (SSRF)	21-Aug-20	5	Server-Side Request Forgery in Canvas LMS 2020-07-29 allows a remote, unauthenticated attacker to cause the Canvas application to perform HTTP GET requests to arbitrary domains. **CVE ID : CVE-2020-5775**	N/A	A-INS-CANV-070920/167
irrelon					
\@irrelon\/path					
Improper Input Validation	18-Aug-20	7.5	The package irrelon-path before 4.7.0; the package @irrelon/path before 4.7.0 are vulnerable to Prototype Pollution via the set, unSet,	N/A	A-IRR-\@IR-070920/168

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
			pushVal and pullVal functions. **CVE ID : CVE-2020-7708**		
irrelon-path					
Improper Input Validation	18-Aug-20	7.5	The package irrelon-path before 4.7.0; the package @irrelon/path before 4.7.0 are vulnerable to Prototype Pollution via the set, unSet, pushVal and pullVal functions. **CVE ID : CVE-2020-7708**	N/A	A-IRR-IRRE-070920/169
ISC					
bind					
Reachable Assertion	21-Aug-20	5	In BIND 9.15.6 -> 9.16.5, 9.17.0 -> 9.17.3, An attacker who can establish a TCP connection with the server and send data on that connection can exploit this to trigger the assertion failure, causing the server to exit. **CVE ID : CVE-2020-8620**	https://kb.isc.org/docs/cve-2020-8620, https://security.netapp.com/advisory/ntap-20200827-0003/, https://www.synology.com/security/advisory/Synology_SA_20_19	A-ISC-BIND-070920/170
Improper Input Validation	21-Aug-20	4.3	In BIND 9.14.0 -> 9.16.5, 9.17.0 -> 9.17.3, If a server is configured with both QNAME minimization and 'forward first' then an attacker who can send queries to it may be able to trigger the condition that will cause the server to crash. Servers that 'forward only' are not affected.	https://kb.isc.org/docs/cve-2020-8621, https://security.netapp.com/advisory/ntap-20200827-0003/, https://ww	A-ISC-BIND-070920/171

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-2020-8621	w.synology.com/security/advisory/Synology_SA_20_19	
Reachable Assertion	21-Aug-20	4	In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit. Alternately, an off-path attacker would have to correctly guess when a TSIG-signed request was sent, along with other characteristics of the packet and message, and spoof a truncated response to trigger an assertion failure, causing the server to exit. **CVE ID : CVE-2020-8622**	https://kb.isc.org/docs/cve-2020-8622, https://security.netapp.com/advisory/ntap-20200827-0003/, https://www.synology.com/security/advisory/Synology_SA_20_19	A-ISC-BIND-070920/172
Improper Privilege Management	21-Aug-20	4.3	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND that was	https://kb.isc.org/docs/cve-2020-8623, https://security.netapp.com/advisory/ntap-20200827-0003/, https://ww	A-ISC-BIND-070920/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			built with "--enable-native-pkcs11" * be signing one or more zones with an RSA key * be able to receive queries from a possible attacker **CVE ID : CVE-2020-8623**	w.synology.com/security/advisory/Synology_SA_20_19	
Improper Privilege Management	21-Aug-20	4	In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could abuse these unintended additional privileges to update other contents of the zone. **CVE ID : CVE-2020-8624**	https://kb.isc.org/docs/cve-2020-8624, https://security.netapp.com/advisory/ntap-20200827-0003/, https://www.synology.com/security/advisory/Synology_SA_20_19	A-ISC-BIND-070920/174
Joomla					
joomla\!					
URL Redirection to Untrusted Site ('Open Redirect')	26-Aug-20	5.8	An issue was discovered in Joomla! before 3.9.21. Lack of input validation in the vote feature of com_content leads to an open redirect. **CVE ID : CVE-2020-24598**	N/A	A-JOO-JOOM-070920/175
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	4.3	An issue was discovered in Joomla! before 3.9.21. Lack of escaping in mod_latestactions allows XSS attacks. **CVE ID : CVE-2020-24599**	N/A	A-JOO-JOOM-070920/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
lightbend					
play_framework					
Cross-Site Request Forgery (CSRF)	17-Aug-20	4.3	In Play Framework 2.6.0 through 2.8.1, the CSRF filter can be bypassed by making CORS simple requests with content types that contain parameters that can't be parsed. **CVE ID : CVE-2020-12480**	N/A	A-LIG-PLAY-070920/177
linux-cmdline_project					
linux-cmdline					
Improper Input Validation	17-Aug-20	7.5	The package linux-cmdline before 1.0.1 are vulnerable to Prototype Pollution via the constructor. **CVE ID : CVE-2020-7704**	N/A	A-LIN-LINU-070920/178
LUA					
lua					
NULL Pointer Dereference	17-Aug-20	5	ldebug.c in Lua 5.4.0 attempts to access debug information via the line hook of a stripped function, leading to a NULL pointer dereference. **CVE ID : CVE-2020-24369**	N/A	A-LUA-LUA-070920/179
Integer Underflow (Wrap or Wraparound)	17-Aug-20	5	ldebug.c in Lua 5.4.0 allows a negation overflow and segmentation fault in getlocal and setlocal, as demonstrated by getlocal(3,2^31). **CVE ID : CVE-2020-24370**	N/A	A-LUA-LUA-070920/180
Release of Invalid Pointer or Reference	17-Aug-20	5	lgc.c in Lua 5.4.0 mishandles the interaction between barriers and the sweep phase, leading to a memory access violation involving	N/A	A-LUA-LUA-070920/181

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
			collectgarbage. **CVE ID : CVE-2020-24371**		
luajit					
luajit					
Out-of-bounds Read	17-Aug-20	5	LuaJIT through 2.1.0-beta3 has an out-of-bounds read in lj_err_run in lj_err.c. **CVE ID : CVE-2020-24372**	N/A	A-LUA-LUAJ-070920/182
Magento					
magento					
Information Exposure Through Discrepancy	20-Aug-20	4	OpenMage LTS before versions 19.4.6 and 20.0.2 allows attackers to circumvent the `fromkey protection` in the Admin Interface and increases the attack surface for Cross Site Request Forgery attacks. This issue is related to Adobe's CVE-2020-9690. It is patched in versions 19.4.6 and 20.0.2. **CVE ID : CVE-2020-15151**	https://github.com/OpenMage/magento-lts/security/advisories/GHSA-crf2-xm6x-46p6	A-MAG-MAGE-070920/183
Marvell					
qconvergeconsole					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Aug-20	5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Marvell QConvergeConsole 5.5.0.64. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getFileUploadBytes method of the FlashValidatorServiceImpl class. The issue results from the lack of proper validation	N/A	A-MAR-QCON-070920/184

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
			of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10497. **CVE ID : CVE-2020-15640**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Aug-20	5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Marvell QConvergeConsole 5.5.0.64. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getFileUploadBytes method of the FlashValidatorServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10499. **CVE ID : CVE-2020-15641**	N/A	A-MAR-QCON-070920/185
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Aug-20	9	This vulnerability allows remote attackers to execute arbitrary code on affected installations of installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within	N/A	A-MAR-QCON-070920/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the isHPSmartComponent method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10501. **CVE ID : CVE-2020-15642**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Aug-20	9	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the saveAsText method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10549. **CVE ID : CVE-2020-15643**	N/A	A-MAR-QCON-070920/187
Improper Limitation of a Pathname to a Restricted	25-Aug-20	9	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64.	N/A	A-MAR-QCON-070920/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the setAppFileBytes method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10550. **CVE ID : CVE-2020-15644**		
Unrestricted Upload of File with Dangerous Type	25-Aug-20	9	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the getFileFromURL method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10553. **CVE ID : CVE-2020-15645**	N/A	A-MAR-QCON-070920/189
Improper	25-Aug-20	9	This vulnerability allows	N/A	A-MAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the writeObjectToConfigFile method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10565. **CVE ID : CVE-2020-17387**		QCON-070920/190
Exposed Dangerous Method or Function	25-Aug-20	9	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the Tomcat configuration file. The issue results from the lack of proper restriction to the Tomcat admin console. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was	N/A	A-MAR-QCON-070920/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZDI-CAN-10799. **CVE ID : CVE-2020-17388**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Aug-20	9	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the decryptFile method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10502. **CVE ID : CVE-2020-17389**	N/A	A-MAR-QCON-070920/192
Mcafee					
total_protection					
Improper Privilege Management	21-Aug-20	3.3	Privilege Escalation vulnerability in the installer in McAfee McAfee Total Protection (MTP) trial prior to 4.0.161.1 allows local users to change files that are part of write protection rules via manipulating symbolic links to redirect a McAfee file operations to an unintended file. **CVE ID : CVE-2020-7310**	http://service.mcafee.com/FAQDocument.aspx?&id=TS103067	A-MCA-TOTA-070920/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Microfocus					
arcsight_management_center					
N/A	19-Aug-20	5	Denial of service vulnerability on Micro Focus ArcSight Management Center. Affecting all versions prior to version 2.9.5. The vulnerability could cause the server to become unavailable, causing a denial of service. **CVE ID : CVE-2020-11848**	N/A	A-MIC-ARCS-070920/194
Microsoft					
365_apps					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Outlook when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1483**	N/A	A-MIC-365_-070920/195
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when attaching files to Outlook messages, aka 'Microsoft Outlook Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1493**	N/A	A-MIC-365_-070920/196
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1495,	N/A	A-MIC-365_-070920/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1496, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1494**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1496, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1495**	N/A	A-MIC-365_-070920/198
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1495, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1496**	N/A	A-MIC-365_-070920/199
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1497**	N/A	A-MIC-365_-070920/200
Improper Restriction of Operations within the	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to	N/A	A-MIC-365_-070920/201

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
Bounds of a Memory Buffer			properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1495, CVE-2020-1496, CVE-2020-1504. **CVE ID : CVE-2020-1498**		
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1503, CVE-2020-1583. **CVE ID : CVE-2020-1502**	N/A	A-MIC-365_-070920/202
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1583. **CVE ID : CVE-2020-1503**	N/A	A-MIC-365_-070920/203
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1563**	N/A	A-MIC-365_-070920/204
Improper Privilege	17-Aug-20	9.3	An elevation of privilege vulnerability exists in the way	N/A	A-MIC-365_-

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
Management			that Microsoft Office Click-to-Run (C2R) components handle objects in memory, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1581**		070920/205
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory, aka 'Microsoft Access Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1582**	N/A	A-MIC-365_-070920/206
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1503. **CVE ID : CVE-2020-1583**	N/A	A-MIC-365_-070920/207
sharepoint_designer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1580. **CVE ID : CVE-2020-1573**	N/A	A-MIC-SHAR-070920/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
office_web_apps					
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1583. **CVE ID : CVE-2020-1503**	N/A	A-MIC-OFFI-070920/209
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1503. **CVE ID : CVE-2020-1583**	N/A	A-MIC-OFFI-070920/210
access					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory, aka 'Microsoft Access Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1582**	N/A	A-MIC-ACCE-070920/211
chakracore					
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine	N/A	A-MIC-CHAK-070920/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1570. **CVE ID : CVE-2020-1555**		
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1570. **CVE ID : CVE-2020-1555**	N/A	A-MIC-EDGE-070920/213
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1568**	N/A	A-MIC-EDGE-070920/214
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1569**	N/A	A-MIC-EDGE-070920/215
office					
Improper Restriction of Operations within the Bounds of a	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Outlook when the software fails to properly handle objects in memory,	N/A	A-MIC-OFFI-070920/216

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
Memory Buffer			aka 'Microsoft Outlook Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1483**		
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when attaching files to Outlook messages, aka 'Microsoft Outlook Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1493**	N/A	A-MIC-OFFI-070920/217
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1495, CVE-2020-1496, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1494**	N/A	A-MIC-OFFI-070920/218
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1496, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1495**	N/A	A-MIC-OFFI-070920/219
Improper Restriction of Operations within the	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to	N/A	A-MIC-OFFI-070920/220

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
Bounds of a Memory Buffer			properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1495, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1496**		
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1497**	N/A	A-MIC-OFFI-070920/221
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1495, CVE-2020-1496, CVE-2020-1504. **CVE ID : CVE-2020-1498**	N/A	A-MIC-OFFI-070920/222
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1503, CVE-2020-1583. **CVE ID : CVE-2020-1502**	N/A	A-MIC-OFFI-070920/223

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	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1583. **CVE ID : CVE-2020-1503**	N/A	A-MIC-OFFI-070920/224
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1563**	N/A	A-MIC-OFFI-070920/225
Improper Privilege Management	17-Aug-20	9.3	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) components handle objects in memory, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1581**	N/A	A-MIC-OFFI-070920/226
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory, aka 'Microsoft Access Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1582**	N/A	A-MIC-OFFI-070920/227
Information	17-Aug-20	4.3	An information disclosure vulnerability exists when	N/A	A-MIC-OFFI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1503. **CVE ID : CVE-2020-1583**		070920/228
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**	N/A	A-MIC-INTE-070920/229
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**	N/A	A-MIC-INTE-070920/230
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-	N/A	A-MIC-INTE-070920/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1555. **CVE ID : CVE-2020-1570**		
.net_framework					
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	A-MIC-.NET-070920/232
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	A-MIC-.NET-070920/233
visual_studio_2017					
Improper Input Validation	17-Aug-20	5	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2020-1597**	N/A	A-MIC-VISU-070920/234
asp.net_core					
Improper Input Validation	17-Aug-20	5	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2020-1597**	N/A	A-MIC-ASP.-070920/235
sharepoint_server					

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 Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1496, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1495**	N/A	A-MIC-SHAR-070920/236
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1500, CVE-2020-1501. **CVE ID : CVE-2020-1499**	N/A	A-MIC-SHAR-070920/237
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1499, CVE-2020-1501. **CVE ID : CVE-2020-1500**	N/A	A-MIC-SHAR-070920/238
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected	N/A	A-MIC-SHAR-070920/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1499, CVE-2020-1500. **CVE ID : CVE-2020-1501**		
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1503, CVE-2020-1583. **CVE ID : CVE-2020-1502**	N/A	A-MIC-SHAR-070920/240
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1583. **CVE ID : CVE-2020-1503**	N/A	A-MIC-SHAR-070920/241
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1505**	N/A	A-MIC-SHAR-070920/242
Improper Neutralization of Input During Web	17-Aug-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a	N/A	A-MIC-SHAR-070920/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1580. **CVE ID : CVE-2020-1573**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1573. **CVE ID : CVE-2020-1580**	N/A	A-MIC-SHAR-070920/244
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1503. **CVE ID : CVE-2020-1583**	N/A	A-MIC-SHAR-070920/245
outlook					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Outlook when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1483**	N/A	A-MIC-OUTL-070920/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when attaching files to Outlook messages, aka 'Microsoft Outlook Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1493**	N/A	A-MIC-OUTL-070920/247
word					
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1583. **CVE ID : CVE-2020-1503**	N/A	A-MIC-WORD-070920/248
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1503. **CVE ID : CVE-2020-1583**	N/A	A-MIC-WORD-070920/249
sharepoint_enterprise_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1496, CVE-2020-	N/A	A-MIC-SHAR-070920/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1498, CVE-2020-1504. **CVE ID : CVE-2020-1495**		
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1500, CVE-2020-1501. **CVE ID : CVE-2020-1499**	N/A	A-MIC-SHAR-070920/251
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1499, CVE-2020-1501. **CVE ID : CVE-2020-1500**	N/A	A-MIC-SHAR-070920/252
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1499, CVE-2020-1500. **CVE ID : CVE-2020-1501**	N/A	A-MIC-SHAR-070920/253
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its	N/A	A-MIC-SHAR-070920/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1583. **CVE ID : CVE-2020-1503**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1505**	N/A	A-MIC-SHAR-070920/255
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1580. **CVE ID : CVE-2020-1573**	N/A	A-MIC-SHAR-070920/256
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1573. **CVE ID : CVE-2020-1580**	N/A	A-MIC-SHAR-070920/257
Information	17-Aug-20	4.3	An information disclosure vulnerability exists when	N/A	A-MIC-SHAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1503. **CVE ID : CVE-2020-1583**		070920/258
office_online_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1496, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1495**	N/A	A-MIC-OFFI-070920/259
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1503, CVE-2020-1583. **CVE ID : CVE-2020-1502**	N/A	A-MIC-OFFI-070920/260
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502,	N/A	A-MIC-OFFI-070920/261

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-2020-1583. **CVE ID : CVE-2020-1503**		
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Word improperly discloses the contents of its memory, aka 'Microsoft Word Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1502, CVE-2020-1503. **CVE ID : CVE-2020-1583**	N/A	A-MIC-OFFI-070920/262
sharepoint_foundation					
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1500, CVE-2020-1501. **CVE ID : CVE-2020-1499**	N/A	A-MIC-SHAR-070920/263
Improper Input Validation	17-Aug-20	5.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1499, CVE-2020-1500. **CVE ID : CVE-2020-1501**	N/A	A-MIC-SHAR-070920/264
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server	N/A	A-MIC-SHAR-070920/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fails to properly handle objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1505**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1580. **CVE ID : CVE-2020-1573**	N/A	A-MIC-SHAR-070920/266
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1573. **CVE ID : CVE-2020-1580**	N/A	A-MIC-SHAR-070920/267
excel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1495, CVE-2020-1496, CVE-2020-	N/A	A-MIC-EXCE-070920/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1498, CVE-2020-1504. **CVE ID : CVE-2020-1494**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1496, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1495**	N/A	A-MIC-EXCE-070920/269
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1495, CVE-2020-1498, CVE-2020-1504. **CVE ID : CVE-2020-1496**	N/A	A-MIC-EXCE-070920/270
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1497**	N/A	A-MIC-EXCE-070920/271
Improper Restriction of Operations within the Bounds of a	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in	N/A	A-MIC-EXCE-070920/272

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
Memory Buffer			memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1495, CVE-2020-1496, CVE-2020-1504. **CVE ID : CVE-2020-1498**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1494, CVE-2020-1495, CVE-2020-1496, CVE-2020-1498. **CVE ID : CVE-2020-1504**	N/A	A-MIC-EXCE-070920/273
visual_studio_code					
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists in Visual Studio Code when it process environment variables after opening a project, aka 'Visual Studio Code Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0604**	N/A	A-MIC-VISU-070920/274
sql_server_management_studio					
Improper Input Validation	17-Aug-20	2.1	A denial of service vulnerability exists when Microsoft SQL Server Management Studio (SSMS) improperly handles files, aka 'Microsoft SQL Server Management Studio Denial of Service Vulnerability'. **CVE ID : CVE-2020-1455**	N/A	A-MIC-SQL_-070920/275

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
visual_studio_2019					
Improper Input Validation	17-Aug-20	5	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2020-1597**	N/A	A-MIC-VISU-070920/276
dynamics_365					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. **CVE ID : CVE-2020-1591**	N/A	A-MIC-DYNA-070920/277
dynamics_365_for_finance_and_operations					
Improper Input Validation	17-Aug-20	6	A remote code execution vulnerability exists in Microsoft Dynamics 365 for Finance and Operations (on-premises) version 10.0.11, aka 'Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1182**	N/A	A-MIC-DYNA-070920/278
Mongodb					
mongodb					
Improper Handling of Exceptional Conditions	21-Aug-20	4	A user authorized to perform database queries may cause denial of service by issuing specially crafted queries, which violate an invariant in	N/A	A-MON-MONG-070920/279

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 query subsystem's support for geoNear. This issue affects: MongoDB Inc. MongoDB Server v4.5 versions prior to 4.5.1; v4.4 versions prior to 4.4.0-rc7; v4.2 versions prior to 4.2.8; v4.0 versions prior to 4.0.19. **CVE ID : CVE-2020-7923**		
naviwebs					
navigatecms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	3.5	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) via the module "Shop." **CVE ID : CVE-2020-23654**	N/A	A-NAV-NAVI-070920/280
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	3.5	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Configuration." **CVE ID : CVE-2020-23655**	N/A	A-NAV-NAVI-070920/281
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	3.5	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Content." **CVE ID : CVE-2020-23656**	N/A	A-NAV-NAVI-070920/282
Improper Neutralization of Input During Web	26-Aug-20	3.5	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Configuration."	N/A	A-NAV-NAVI-070920/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2020-23657**		
Net-snmp					
net-snmp					
Improper Link Resolution Before File Access ('Link Following')	20-Aug-20	7.2	Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following. **CVE ID : CVE-2020-15861**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=966599, https://github.com/net-snmp/net-snmp/commit/4fd9a450444a434a993bc72f7c3486ccce41f602, https://github.com/net-snmp/net-snmp/issues/145	A-NET-NET--070920/284
Improper Privilege Management	20-Aug-20	7.2	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root. **CVE ID : CVE-2020-15862**	https://github.com/net-snmp/net-snmp/commit/77f6c60f57dba0aaea5d8ef1dd94bcd0c8e6d205, https://salsa.debian.org/debian/net-snmp/-/commit/fa	A-NET-NET--070920/285

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
				d8725402752746daf0a751dcff19eb6aeab52e	
Nextcloud					
nextcloud					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-20	3.5	A cross-site scripting error in Nextcloud Desktop client 2.6.4 allowed to present any html (including local links) when responding with invalid data on the login attempt. **CVE ID : CVE-2020-8189**	N/A	A-NEX-NEXT-070920/286
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-20	7.1	Missing sanitization of a server response in Nextcloud Desktop Client 2.6.4 for Linux allowed a malicious Nextcloud Server to store files outside of the dedicated sync directory. **CVE ID : CVE-2020-8227**	N/A	A-NEX-NEXT-070920/287
Out-of-bounds Write	17-Aug-20	2.1	A memory corruption vulnerability exists in NextCloud Desktop Client v2.6.4 where missing ASLR and DEP protections in for windows allowed to corrupt memory. **CVE ID : CVE-2020-8230**	N/A	A-NEX-NEXT-070920/288
nexusdb					
nexusdb					
Improper Limitation of a Pathname to a Restricted Directory	21-Aug-20	5	NexusQA NexusDB before 4.50.23 allows the reading of files via ../ directory traversal. **CVE ID : CVE-2020-24571**	N/A	A-NEX-NEXU-070920/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')					
nis-utils_project					
nis-utils					
Uncontrolled Resource Consumption	17-Aug-20	7.5	All versions of package nis-utils are vulnerable to Prototype Pollution via the setValue function. **CVE ID : CVE-2020-7703**	N/A	A-NIS-NIS--070920/290
nodebb					
nodebb					
Improper Privilege Management	20-Aug-20	6.5	NodeBB before version 1.14.3 has a bug introduced in version 1.12.2 in the validation logic that makes it possible to change the password of any user on a running NodeBB forum by sending a specially crafted socket.io call to the server. This could lead to a privilege escalation event due via an account takeover. As a workaround you may cherry-pick the following commit from the project's repository to your running instance of NodeBB: 16cee1b03ba3eee177834a1fdac4aa8a12b39d2a. This is fixed in version 1.14.3. **CVE ID : CVE-2020-15149**	https://github.com/NodeBB/NodeBB/security/advisories/GHSA-hr66-c8pg-5mg7	A-NOD-NODE-070920/291
online_shopping_alphaware_project					
online_shopping_alphaware					
Improper Neutralization of Special Elements	17-Aug-20	7.5	A SQL injection vulnerability in SourceCodester Online Shopping Alphaware 1.0 allows remote	N/A	A-ONL-ONLI-070920/292

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
used in an SQL Command ('SQL Injection')			unauthenticated attackers to bypass the authentication process via email and password parameters. **CVE ID : CVE-2020-24208**		
openmage					
openmage_long_term_support					
Information Exposure Through Discrepancy	20-Aug-20	4	OpenMage LTS before versions 19.4.6 and 20.0.2 allows attackers to circumvent the `fromkey protection` in the Admin Interface and increases the attack surface for Cross Site Request Forgery attacks. This issue is related to Adobe's CVE-2020-9690. It is patched in versions 19.4.6 and 20.0.2. **CVE ID : CVE-2020-15151**	https://github.com/OpenMage/magento-lts/security/advisories/GHSA-crf2-xm6x-46p6	A-OPE-OPEN-070920/293
Osticket					
osticket					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	3.5	osTicket before 1.14.3 allows XSS because include/staff/banrule.inc.php has an unvalidated echo $info['notes'] call. **CVE ID : CVE-2020-16193**	https://github.com/osTicket/osTicket/pull/5616/commits/fb570820ef1138776f929a179906e1d8089179d9	A-OST-OSTI-070920/294
Parallels					
parallels_desktop					
Untrusted Pointer Dereference	25-Aug-20	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.3-47255. An	N/A	A-PAR-PARA-070920/295

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
			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 handler for HOST_IOCTL_SET_KERNEL_SYMBOLS in the prl_hypervisor kext. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-10519. **CVE ID : CVE-2020-17392**		
Improper Input Validation	25-Aug-20	2.1	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.3-47255. 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 prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result a pointer to be leaked after the handler is done. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context	N/A	A-PAR-PARA-070920/296

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
			of the kernel. Was ZDI-CAN-10520. **CVE ID : CVE-2020-17393**		
Integer Underflow (Wrap or Wraparound)	25-Aug-20	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. 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 prl_naptd process. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11134. **CVE ID : CVE-2020-17395**	N/A	A-PAR-PARA-070920/297
Integer Overflow or Wraparound	25-Aug-20	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. 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 prl_hypervisor module. The issue results from the lack of proper validation of user-supplied data, which can	N/A	A-PAR-PARA-070920/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 kernel. Was ZDI-CAN-11217. **CVE ID : CVE-2020-17396**		
Improper Validation of Array Index	25-Aug-20	2.1	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.4. 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 prl_hypervisor kext. 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 arbitrary code in the context of the kernel. Was ZDI-CAN-11302. **CVE ID : CVE-2020-17398**	N/A	A-PAR-PARA-070920/299
Improper Validation of Array Index	25-Aug-20	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	N/A	A-PAR-PARA-070920/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The specific flaw exists within the prl_hypervisor kext. 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-11303. **CVE ID : CVE-2020-17399**		
Improper Validation of Array Index	25-Aug-20	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. 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 prl_hypervisor kext. 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 vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11304. **CVE ID : CVE-2020-17400**	N/A	A-PAR-PARA-070920/301
Improper Validation of Array Index	25-Aug-20	2.1	This vulnerability allows local attackers to disclose sensitive informations on affected installations of Parallels Desktop 15.1.4. An attacker	N/A	A-PAR-PARA-070920/302

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
			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 read past the end of an allocated array. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11363. **CVE ID : CVE-2020-17401**		
Philips					
dreammapper					
Information Exposure Through Log Files	21-Aug-20	5	Philips DreamMapper, Version 2.24 and prior. Information written to log files can give guidance to a potential attacker. **CVE ID : CVE-2020-14518**	N/A	A-PHI-DREA-070920/303
Phpbb					
phpbb					
Server-Side Request Forgery (SSRF)	17-Aug-20	5	A vulnerability exists in phpBB <v3.2.10 and <v3.3.1 which allowed remote image dimensions check to be used to SSRF. **CVE ID : CVE-2020-8226**	N/A	A-PHP-PHPB-070920/304
Postgresql					
postgresql					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Aug-20	6.5	It was found that PostgreSQL versions before 12.4, before 11.9 and before 10.14 did not properly sanitize the search_path during logical replication. An authenticated attacker could use this flaw in an attack similar to CVE-2018-1058, in order to execute arbitrary SQL command in the context of the user used for replication. **CVE ID : CVE-2020-14349**	N/A	A-POS-POST-070920/305
Untrusted Search Path	24-Aug-20	4.4	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension. This affects PostgreSQL versions before 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23. **CVE ID : CVE-2020-14350**	N/A	A-POS-POST-070920/306
property-expr_project					
property-expr					
Improper Input Validation	18-Aug-20	7.5	The package property-expr before 2.0.3 are vulnerable to Prototype Pollution via the setter function. **CVE ID : CVE-2020-7707**	N/A	A-PRO-PROP-070920/307
rangee					
rangeeos					
Improper	20-Aug-20	7.5	The Kommbox component in	N/A	A-RAN-RANG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Rangee GmbH RangeeOS 8.0.4 is vulnerable to Remote Code Execution due to untrusted user supplied input being passed to the command line without sanitization. **CVE ID : CVE-2020-16279**		070920/308
Insufficiently Protected Credentials	20-Aug-20	2.1	Multiple Rangee GmbH RangeeOS 8.0.4 modules store credentials in plaintext including credentials of users for several external facing administrative services, domain joined users, and local administrators. To exploit the vulnerability a local attacker must have access to the underlying operating system. **CVE ID : CVE-2020-16280**	N/A	A-RAN-RANG-070920/309
Improper Encoding or Escaping of Output	20-Aug-20	4.6	The Kommbox component in Rangee GmbH RangeeOS 8.0.4 could allow a local authenticated attacker to escape from the restricted environment and execute arbitrary code due to unrestricted context menus being accessible. **CVE ID : CVE-2020-16281**	N/A	A-RAN-RANG-070920/310
Ritecms					
ritecms					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-Aug-20	9	An issue was discovered in RiteCMS 2.2.1. An authenticated user can directly execute system commands by uploading a php web shell in the "Filemanager" section.	N/A	A-RIT-RITE-070920/311

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
Injection')			**CVE ID : CVE-2020-23934**		
rocket.chat					
rocket.chat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-20	4.3	Rocket.Chat through 3.4.2 allows XSS where an attacker can send a specially crafted message to a channel or in a direct message to the client which results in remote code execution on the client side. **CVE ID : CVE-2020-15926**	N/A	A-ROC-ROCK-070920/312
safe-eval_project					
safe-eval					
Improper Privilege Management	21-Aug-20	7.5	This affects all versions of package safe-eval. It is possible for an attacker to run an arbitrary command on the host machine. **CVE ID : CVE-2020-7710**	N/A	A-SAF-SAFE-070920/313
shopxo					
shopxo					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	ShopXO v1.8.1 has a command execution vulnerability. Attackers can use this vulnerability to execute arbitrary commands and gain control of the server. **CVE ID : CVE-2020-24220**	N/A	A-SHO-SHOP-070920/314
silabs					
bluetooth_low_energy_software_development_kit					
Buffer Copy without Checking Size of Input ('Classic	20-Aug-20	5.8	Silicon Labs Bluetooth Low Energy SDK before 2.13.3 has a buffer overflow via packet data. This is an over-the-air remote code execution	N/A	A-SIL-BLUE-070920/315

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
Buffer Overflow')			vulnerability in Bluetooth LE in EFR32 SoCs and associated modules running Bluetooth SDK, supporting Central or Observer roles. **CVE ID : CVE-2020-15531**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Aug-20	3.3	Silicon Labs Bluetooth Low Energy SDK before 2.13.3 has a buffer overflow via packet data. This is an over-the-air denial of service vulnerability in Bluetooth LE in EFR32 SoCs and associated modules running Bluetooth SDK, supporting Central or Observer roles. **CVE ID : CVE-2020-15532**	N/A	A-SIL-BLUE-070920/316
snmptt					
snmptt					
Improper Check for Dropped Privileges	16-Aug-20	7.5	SNMPTT before 1.4.2 allows attackers to execute shell code via EXEC, PREXEC, or unknown_trap_exec. **CVE ID : CVE-2020-24361**	N/A	A-SNM-SNMP-070920/317
Softing					
opc					
Uncontrolled Resource Consumption	25-Aug-20	5	Softing Industrial Automation all versions prior to the latest build of version 4.47.0, The affected product is vulnerable to uncontrolled resource consumption, which may allow an attacker to cause a denial-of-service condition. **CVE ID : CVE-2020-14522**	N/A	A-SOF-OPC-070920/318
Out-of-bounds Write	25-Aug-20	7.5	Softing Industrial Automation all versions prior to the latest	N/A	A-SOF-OPC-070920/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			build of version 4.47.0, The affected product is vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2020-14524**		
soluzioneglobale					
ecommerce_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-20	7.5	SQL injection can occur in Soluzione Globale Ecommerce CMS v1 via the parameter " offerta.php" **CVE ID : CVE-2020-23978**	N/A	A-SOL-ECOM-070920/320
stimulsoft					
reports					
Improper Input Validation	18-Aug-20	9.3	A Remote Code Execution vulnerability in Stimulsoft (aka Stimulsoft Reports) 2013.1.1600.0 allows an attacker to encode C# scripts as base-64 in the report XML file so that they will be compiled and executed on the server that processes this file. This can be used to fully compromise the server. **CVE ID : CVE-2020-15865**	N/A	A-STI-REPO-070920/321
student_management_system_project					
student_management_system					
Improper Authentication	20-Aug-20	7.5	Kabir Alhasan Student Management System 1.0 is vulnerable to Authentication Bypass via "Username:	N/A	A-STU-STUD-070920/322

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
			admin'# && Password: (Write Something)". **CVE ID : CVE-2020-23935**		
sylius					
syliusresourcebundle					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Aug-20	6.5	In SyliusResourceBundle before versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4, rrequest parameters injected inside an expression evaluated by `symfony/expression-language` package haven't been sanitized properly. This allows the attacker to access any public service by manipulating that request parameter, allowing for Remote Code Execution. This issue has been patched for versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4. Versions prior to 1.3 were not patched. **CVE ID : CVE-2020-15143**	https://github.com/Sylius/SyliusResourceBundle/security/advisories/GHSA-p4pj-9g59-4ppv	A-SYL-SYLI-070920/323
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Aug-20	6.5	In SyliusResourceBundle before versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4, request parameters injected inside an expression evaluated by `symfony/expression-language` package haven't been sanitized properly. This allows the attacker to access any public service by manipulating that request parameter, allowing for Remote Code Execution. This issue has been patched for versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4. Versions prior to	https://github.com/Sylius/SyliusResourceBundle/security/advisories/GHSA-h6m7-j4h3-9rf5	A-SYL-SYLI-070920/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.3 were not patched. **CVE ID : CVE-2020-15146**		
Sysax					
multi_server					
Unrestricted Upload of File with Dangerous Type	19-Aug-20	4	When uploading a file in Sysax Multi Server 6.90, an authenticated user can modify the filename="" parameter in the uploadfile_name1.htm form to a length of 368 or more bytes. This will create a buffer overflow condition, causing the application to crash. **CVE ID : CVE-2020-23574**	N/A	A-SYS-MULT-070920/325
techkshetrainfo					
savsoft_quiz					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-20	4.3	TechKshetra Info Solutions Pvt. Ltd Savsoft Quiz 5 has XSS which can result in an attacker injecting the XSS payload in the User Registration section and each time the admin visits the manage user section from the admin panel, the XSS triggers and the attacker can steal the cookie via crafted payload. **CVE ID : CVE-2020-24609**	N/A	A-TEC-SAVS-070920/326
templ8_project					
templ8					
Uncontrolled Resource Consumption	17-Aug-20	7.5	All versions of package templ8 are vulnerable to Prototype Pollution via the parse function. **CVE ID : CVE-2020-7702**	N/A	A-TEM-TEMP-070920/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Tenable					
nessus					
Insufficient Session Expiration	21-Aug-20	3.6	Nessus versions 8.11.0 and earlier were found to maintain sessions longer than the permitted period in certain scenarios. The lack of proper session expiration could allow attackers with local access to login into an existing browser session. **CVE ID : CVE-2020-5774**	N/A	A-TEN-NESS-070920/328
teradici					
pcoip_management_console					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-20	4.3	Reflected Cross Site Scripting in Teradici PCoIP Management Console prior to 20.07 could allow an attacker to take over the user's active session if the user is exposed to a malicious payload. **CVE ID : CVE-2020-13183**	N/A	A-TER-PCOI-070920/329
Tibco					
data_virtualization					
Information Exposure	18-Aug-20	4	The TIBCO Data Virtualization Server component of TIBCO Software Inc.'s TIBCO Data Virtualization and TIBCO Data Virtualization for AWS Marketplace contains a vulnerability that theoretically allows a malicious authenticated user to download any arbitrary file from the affected system. The user must be authenticated and have privileges required to monitor the server in an	http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2020/08/tibco-security-advisory-august-18-2020-tibco-	A-TIB-DATA-070920/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operational capacity. Affected releases are TIBCO Software Inc.'s TIBCO Data Virtualization: versions 7.0.8 and below, versions 8.0.0, 8.1.0, 8.1.1, and 8.2.0 and TIBCO Data Virtualization for AWS Marketplace: versions 8.2.0 and below. **CVE ID : CVE-2020-9415**	data-virtualization	
data_virtualization_for_aws_marketplace					
Information Exposure	18-Aug-20	4	The TIBCO Data Virtualization Server component of TIBCO Software Inc.'s TIBCO Data Virtualization and TIBCO Data Virtualization for AWS Marketplace contains a vulnerability that theoretically allows a malicious authenticated user to download any arbitrary file from the affected system. The user must be authenticated and have privileges required to monitor the server in an operational capacity. Affected releases are TIBCO Software Inc.'s TIBCO Data Virtualization: versions 7.0.8 and below, versions 8.0.0, 8.1.0, 8.1.1, and 8.2.0 and TIBCO Data Virtualization for AWS Marketplace: versions 8.2.0 and below. **CVE ID : CVE-2020-9415**	http://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2020/08/tibco-security-advisory-august-18-2020-tibco-data-virtualization	A-TIB-DATA-070920/331
ui					
edgeswitch_firmware					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in	N/A	A-UI-EDGE-070920/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	A-UI-EDGE-070920/333
vehicle_parking_management_system_project					
vehicle_parking_management_system					
Improper Authentication	20-Aug-20	7.5	PHPGurukul Vehicle Parking Management System 1.0 is vulnerable to Authentication Bypass via "Username: admin'# && Password: (Write Something)". **CVE ID : CVE-2020-23936**	N/A	A-VEH-VEHI-070920/334
Vmware					
vcenter_server					
Improper Authentication	21-Aug-20	5	VMware ESXi and vCenter Server contain a partial denial of service vulnerability in their respective authentication services. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 5.3.	N/A	A-VMW-VCEN-070920/335

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-2020-3976		
app_volumes					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-20	3.5	VMware App Volumes 2.x prior to 2.18.6 and VMware App Volumes 4 prior to 2006 contain a Stored Cross-Site Scripting (XSS) vulnerability. A malicious actor with access to create and edit applications or create storage groups, may be able to inject malicious script which will be executed by a victim's browser when viewing. **CVE ID : CVE-2020-3975**	N/A	A-VMW-APP_-070920/336
cloud_foundation					
Improper Authentication	21-Aug-20	5	VMware ESXi and vCenter Server contain a partial denial of service vulnerability in their respective authentication services. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 5.3. **CVE ID : CVE-2020-3976**	N/A	A-VMW-CLOU-070920/337
webdesi9					
file_manager					
Information Exposure	26-Aug-20	5	mndpsingh287 WP File Manager v6.4 and lower fails to restrict external access to the fm_backups directory with a .htaccess file. This results in the ability for unauthenticated users to browse and download any site backups, which	N/A	A-WEB-FILE-070920/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sometimes include full database backups, that the plugin has taken. **CVE ID : CVE-2020-24312**		
webport_project					
webport					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	3.5	WebPort-v1.19.17121 is affected by Cross Site Scripting (XSS) on the "connections" feature. **CVE ID : CVE-2020-23659**	N/A	A-WEB-WEBP-070920/339
webtareas_project					
webtareas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	3.5	webTareas v2.1 is affected by Cross Site Scripting (XSS) on "Search." **CVE ID : CVE-2020-23660**	N/A	A-WEB-WEBT-070920/340
Wolfssl					
wolfssl					
Improper Input Validation	21-Aug-20	5	An issue was discovered in wolfSSL before 4.5.0. It mishandles the change_cipher_spec (CCS) message processing logic for TLS 1.3. If an attacker sends ChangeCipherSpec messages in a crafted way involving more than one in a row, the server becomes stuck in the ProcessReply() loop, i.e., a denial of service.	https://github.com/wolfSSL/wolfssl/releases/tag/v4.5.0-stable	A-WOL-WOLF-070920/341

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-2020-12457		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Aug-20	6.9	An issue was discovered in wolfSSL before 4.5.0, when single precision is not employed. Local attackers can conduct a cache-timing attack against public key operations. These attackers may already have obtained sensitive information if the affected system has been used for private key operations (e.g., signing with a private key). **CVE ID : CVE-2020-15309**	https://github.com/wolfSSL/wolfssl/releases/tag/v4.5.0-stable	A-WOL-WOLF-070920/342
N/A	21-Aug-20	5	An issue was discovered in the DTLS handshake implementation in wolfSSL before 4.5.0. Clear DTLS application_data messages in epoch 0 do not produce an out-of-order error. Instead, these messages are returned to the application. **CVE ID : CVE-2020-24585**	N/A	A-WOL-WOLF-070920/343
Wso2					
api_manager_analytics					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	5.5	The Management Console in certain WSO2 products allows XXE attacks during EventReceiver updates. This affects API Manager through 3.0.0, API Manager Analytics 2.2.0 and 2.5.0, API Microgateway 2.2.0, Enterprise Integrator 6.2.0 and 6.3.0, and Identity Server Analytics through 5.6.0. **CVE ID : CVE-2020-24591**	N/A	A-WSO-API_-070920/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
api_microgateway					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML External Entity injection (XXE) attacks. **CVE ID : CVE-2020-24589**	N/A	A-WSO-API_-070920/345
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML Entity Expansion attacks. **CVE ID : CVE-2020-24590**	N/A	A-WSO-API_-070920/346
identity_server_analytics					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	5.5	The Management Console in certain WSO2 products allows XXE attacks during EventReceiver updates. This affects API Manager through 3.0.0, API Manager Analytics 2.2.0 and 2.5.0, API Microgateway 2.2.0, Enterprise Integrator 6.2.0 and 6.3.0, and Identity Server Analytics through 5.6.0. **CVE ID : CVE-2020-24591**	N/A	A-WSO-IDEN-070920/347
api_microgatewa					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	5.5	The Management Console in certain WSO2 products allows XXE attacks during EventReceiver updates. This affects API Manager through 3.0.0, API Manager Analytics 2.2.0 and 2.5.0, API Microgateway 2.2.0,	N/A	A-WSO-API_-070920/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Integrator 6.2.0 and 6.3.0, and Identity Server Analytics through 5.6.0. **CVE ID : CVE-2020-24591**		
enterprise_integrator					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	5.5	The Management Console in certain WSO2 products allows XXE attacks during EventReceiver updates. This affects API Manager through 3.0.0, API Manager Analytics 2.2.0 and 2.5.0, API Microgateway 2.2.0, Enterprise Integrator 6.2.0 and 6.3.0, and Identity Server Analytics through 5.6.0. **CVE ID : CVE-2020-24591**	N/A	A-WSO-ENTE-070920/349
api_manager					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML External Entity injection (XXE) attacks. **CVE ID : CVE-2020-24589**	N/A	A-WSO-API_-070920/350
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML Entity Expansion attacks. **CVE ID : CVE-2020-24590**	N/A	A-WSO-API_-070920/351
Improper Restriction of Recursive Entity References in	21-Aug-20	5.5	The Management Console in certain WSO2 products allows XXE attacks during EventReceiver updates. This affects API Manager through	N/A	A-WSO-API_-070920/352

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
DTDs ('XML Entity Expansion')			3.0.0, API Manager Analytics 2.2.0 and 2.5.0, API Microgateway 2.2.0, Enterprise Integrator 6.2.0 and 6.3.0, and Identity Server Analytics through 5.6.0. **CVE ID : CVE-2020-24591**		
xorux					
lpar2rrd					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Aug-20	10	tz.pl on XoruX LPAR2RRD and STOR2RRD 2.70 virtual appliances allows cmd=set&tz=OS command injection via shell metacharacters in a timezone. **CVE ID : CVE-2020-24032**	N/A	A-XOR-LPAR-070920/353
stor2rrd					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Aug-20	10	tz.pl on XoruX LPAR2RRD and STOR2RRD 2.70 virtual appliances allows cmd=set&tz=OS command injection via shell metacharacters in a timezone. **CVE ID : CVE-2020-24032**	N/A	A-XOR-STOR-070920/354
Zulip					
zulip_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-20	4.3	Zulip Server before 2.1.5 allows reflected XSS via the Dropbox webhook. **CVE ID : CVE-2020-12759**	https://blog.zulip.com/2020/06/17/zulip-server-2-1-5-security-release/	A-ZUL-ZULI-070920/355

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 Input Validation	21-Aug-20	5.8	Zulip Server before 2.1.5 allows reverse tabnapping via a topic header link. **CVE ID : CVE-2020-14194**	https://blog.zulip.com/2020/06/17/zulip-server-2-1-5-security-release/	A-ZUL-ZULI-070920/356
Incorrect Authorization	21-Aug-20	5	Zulip Server before 2.1.5 has Incorrect Access Control because 0198_preregistrationuser_invited_as adds the administrator role to invitations. **CVE ID : CVE-2020-14215**	https://blog.zulip.com/2020/06/17/zulip-server-2-1-5-security-release/	A-ZUL-ZULI-070920/357
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Aug-20	6.5	Zulip Server 2.x before 2.1.7 allows eval injection if a privileged attacker were able to write directly to the postgres database, and chose to write a crafted custom profile field value. **CVE ID : CVE-2020-15070**	https://blog.zulip.com/2020/06/26/zulip-server-2-1-7-security-release/	A-ZUL-ZULI-070920/358
Operating System					
Apple					
mac_os					
Out-of-bounds Write	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9693**	N/A	O-APP-MAC_-070920/359
Out-of-bounds Write	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and	N/A	O-APP-MAC_-070920/360

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
			earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9694**		
Incorrect Authorization	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9696**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/361
Information Exposure	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a disclosure of sensitive data vulnerability. Successful exploitation could lead to memory leak. **CVE ID : CVE-2020-9697**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/362
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9698**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/363

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9699**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/364
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9700**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/365
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9701**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/366
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service. **CVE ID : CVE-2020-9702**		
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9703**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/368
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9704**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/369
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9705**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/370
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds	N/A	O-APP-MAC_-070920/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9706**		
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9707**	N/A	O-APP-MAC_-070920/372
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9710**	N/A	O-APP-MAC_-070920/373
Incorrect Authorization	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9712**	N/A	O-APP-MAC_-070920/374
Improper Privilege Management	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and	https://helpx.adobe.com/security/products/acrobat/aps	O-APP-MAC_-070920/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation . **CVE ID : CVE-2020-9714**	b20-48.html	
Use After Free	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9715**	N/A	O-APP-MAC_-070920/376
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9716**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/377
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9717**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/378
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier,	https://helpx.adobe.com/security/products/	O-APP-MAC_-070920/379

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 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9718**	acrobat/apsb20-48.html	
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9719**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/380
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9720**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/381
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9721**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/382
Use After Free	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002,	https://helpx.adobe.com/security	O-APP-MAC_-070920/383

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
			2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9722**	/products/ acrobat/apsb20-48.html	
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9723**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-APP-MAC_-070920/384
Asus					
rt-ac1900p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	4.3	An issue was discovered on ASUS RT-AC1900P routers before 3.0.0.4.385_20253. They allow XSS via spoofed Release Notes on the Firmware Upgrade page. **CVE ID : CVE-2020-15499**	N/A	O-ASU-RT-A-070920/385
cellopoint					
cellos					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Aug-20	9	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly. With the cookie of the system administrator, attackers can inject and remotely execute arbitrary command to manipulate the system.	N/A	O-CEL-CELL-070920/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17384		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Aug-20	5	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly, which allows unauthorized user to launch Path Traversal attack and access arbitrate file on the system. **CVE ID : CVE-2020-17385**	N/A	O-CEL-CELL-070920/387
Server-Side Request Forgery (SSRF)	25-Aug-20	4	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly. With cookie of an authenticated user, attackers can temper with the URL parameter and access arbitrary file on system. **CVE ID : CVE-2020-17386**	N/A	O-CEL-CELL-070920/388
Cisco					
sf302-08pp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the	N/A	O-CIS-SF30-070920/389

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
			switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf302-08mpp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF30-070920/390
sf300-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is	N/A	O-CIS-SF30-070920/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF30-070920/392
sf300-24mp_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF30-070920/393
sf300-24pp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow	N/A	O-CIS-SF30-070920/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF30-070920/395
sf300-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	N/A	O-CIS-SF30-070920/396

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 on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-48pp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF30-070920/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf500-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF50-070920/398
sf500-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	O-CIS-SF50-070920/399

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
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf500-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF50-070920/400
sf500-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	O-CIS-SF50-070920/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500-28_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	O-CIS-SG50-070920/402

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-2020-3363		
sg500-28p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG50-070920/403
sg500-28mpp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	O-CIS-SG50-070920/404

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
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500-52_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG50-070920/405
sg500-52p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	O-CIS-SG50-070920/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500-52mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	O-CIS-SG50-070920/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500x-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG50-070920/408
sg500x-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	O-CIS-SG50-070920/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500x-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG50-070920/410
sg250x-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	O-CIS-SG25-070920/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250x-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	O-CIS-SG25-070920/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250x-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG25-070920/413
sg250x-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	O-CIS-SG25-070920/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-08_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG25-070920/415
sg250-08hp_firmware					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	O-CIS-SG25-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/416
sg250-10p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	O-CIS-SG25-070920/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-18_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG25-070920/418
sg250-26_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	O-CIS-SG25-070920/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-26hp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG25-070920/420

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
sg250-26p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG25-070920/421
sg250-50_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	O-CIS-SG25-070920/422

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
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-50hp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG25-070920/423
sg250-50p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	O-CIS-SG25-070920/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf350-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	O-CIS-SF35-070920/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3363		
sf350-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF35-070920/426
sf350-48mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	O-CIS-SF35-070920/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-10_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/428
sg350-10p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	O-CIS-SG35-070920/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-10mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	O-CIS-SG35-070920/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-28_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/431
sg350-28p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	O-CIS-SG35-070920/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-28mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/433
sx550x-16ft_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	O-CIS-SX55-070920/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sx550x-24ft_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	O-CIS-SX55-070920/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sx550x-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SX55-070920/436
sx550x-52_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	O-CIS-SX55-070920/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg550x-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG55-070920/438
sg550x-24p_firmware					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	O-CIS-SG55-

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
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/439
sg550x-24mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	O-CIS-SG55-070920/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg550x-24mpp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG55-070920/441
sg550x-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	O-CIS-SG55-070920/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg550x-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG55-070920/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg550x-48mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG55-070920/444
staros					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.8	A vulnerability in the IPv6 implementation of Cisco StarOS could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet to an affected device with the goal of reaching the vulnerable	N/A	O-CIS-STAR-070920/445

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
			section of the input buffer. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3500**		
sf200-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF20-070920/446
sf200-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	O-CIS-SF20-070920/447

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
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf200-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	O-CIS-SF20-070920/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sf200-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF20-070920/449
sg200-18_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	O-CIS-SG20-070920/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-26_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG20-070920/451
sg200-26p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	O-CIS-SG20-070920/452

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 Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-50_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	O-CIS-SG20-070920/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-50p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG20-070920/454
sg300-10_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	O-CIS-SG30-070920/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-10mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG30-070920/456
sg300-10mpp_firmware					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	O-CIS-SG30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/457
sg300-10sfp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	O-CIS-SG30-070920/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-10p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG30-070920/459
sg300-10pp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	O-CIS-SG30-070920/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-20_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG30-070920/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-28_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG30-070920/462
sg300-28p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	O-CIS-SG30-070920/463

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
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-28pp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG30-070920/464
sg300-28mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	O-CIS-SG30-070920/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-52_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	O-CIS-SG30-070920/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3363		
sg300-52p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG30-070920/467
sg300-52mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	O-CIS-SG30-070920/468

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
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-08_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF30-070920/469
sf302-08_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	O-CIS-SF30-070920/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf302-08mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	O-CIS-SF30-070920/471

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
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sf302-08p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF30-070920/472
sf550x-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	O-CIS-SF55-070920/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf550x-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF55-070920/474
sf550x-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	O-CIS-SF55-070920/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf550x-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	O-CIS-SF55-070920/476

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. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf550x-48mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF55-070920/477
sg200-50fp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	O-CIS-SG20-070920/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-26fp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG20-070920/479
sg200-10fp_firmware					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	O-CIS-SG20-

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
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/480
sg200-08_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	O-CIS-SG20-070920/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-08p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG20-070920/482
sf200-24fp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	O-CIS-SF20-070920/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500xg-8f8t_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG50-070920/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500x-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG50-070920/485
ios_xr					
Improper Check for Unusual or Exceptional Conditions	17-Aug-20	4.3	A vulnerability in the Border Gateway Protocol (BGP) additional paths feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to prevent authorized users from monitoring the BGP status and cause the BGP process to stop processing new updates, resulting in a denial of service (DOS) condition. The vulnerability is due to an incorrect calculation of lexicographical order when	N/A	O-CIS-IOS_-070920/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			displaying additional path information within Cisco IOS XR Software, which causes an infinite loop. An attacker could exploit this vulnerability by sending a specific BGP update from a BGP neighbor peer session of an affected device; an authorized user must then issue a show bgp command for the vulnerability to be exploited. A successful exploit could allow the attacker to prevent authorized users from properly monitoring the BGP status and prevent BGP from processing new updates, resulting in outdated information in the routing and forwarding tables. **CVE ID : CVE-2020-3449**		
sf250-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	O-CIS-SF25-070920/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf250-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF25-070920/488
sf250-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	O-CIS-SF25-070920/489

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
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf250-48hp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SF25-070920/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg355-10p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/491
sg350xg-2f10_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	O-CIS-SG35-070920/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350xg-24f_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/493
sg350xg-24t_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	O-CIS-SG35-070920/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350xg-48t_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	O-CIS-SG35-070920/495

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-2020-3363		
sg350x-24_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/496
sg350x-24p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	O-CIS-SG35-070920/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350x-24mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/498
sg350x-48_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	O-CIS-SG35-070920/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350x-48p_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	O-CIS-SG35-070920/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350x-48mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SG35-070920/501
sx550x-12f_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	O-CIS-SX55-070920/502

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
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sx550x-24f_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	O-CIS-SX55-070920/503
sf550x-24mp_firmware					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	O-CIS-SF55-070920/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
contiki-ng					
contiki-ng					
Out-of-bounds Write	18-Aug-20	7.5	Buffer overflows were discovered in Contiki-NG 4.4 through 4.5, in the SNMP agent. The function parsing the received SNMP request does not verify the input message's requested variables against the capacity of the internal SNMP engine buffer. If the number of variables in the request exceeds the allocated buffer, a memory write out of the buffer boundaries occurs. This write operation provides a possibility to overwrite other variables allocated in the .bss section by the application.	N/A	O-CON-CONT-070920/505

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
			Because the sender of the frame is in control of the content that will be written beyond the buffer limits, and there is no strict process memory separation, this issue may allow overwriting of sensitive memory areas of an IoT device. **CVE ID : CVE-2020-14934**		
Out-of-bounds Write	18-Aug-20	7.5	Buffer overflows were discovered in Contiki-NG 4.4 through 4.5, in the SNMP bulk get request response encoding function. The function parsing the received SNMP request does not verify the input message's requested variables against the capacity of the internal SNMP engine buffer. When a bulk get request response is assembled, a stack buffer dedicated for OIDs (with a limited capacity) is allocated in snmp_engine_get_bulk(). When snmp_engine_get_bulk() is populating the stack buffer, an overflow condition may occur due to lack of input length validation. This makes it possible to overwrite stack regions beyond the allocated buffer, including the return address from the function. As a result, the code execution path may be redirected to an address provided in the SNMP bulk get payload. If the target architecture uses common	N/A	O-CON-CONT-070920/506

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
			addressing space for program and data memory, it may also be possible to supply code in the SNMP request payload, and redirect the execution path to the remotely injected code, by modifying the function's return address. **CVE ID : CVE-2020-14935**		
Out-of-bounds Write	18-Aug-20	7.5	Buffer overflows were discovered in Contiki-NG 4.4 through 4.5, in the SNMP agent. Functions parsing the OIDs in SNMP requests lack sufficient allocated target-buffer capacity verification when writing parsed OID values. The function snmp_oid_decode_oid() may overwrite memory areas beyond the provided target buffer, when called from snmp_message_decode() upon an SNMP request reception. Because the content of the write operations is externally provided in the SNMP requests, it enables a remote overwrite of an IoT device's memory regions beyond the allocated buffer. This overflow may allow remote overwrite of stack and statically allocated variables memory regions by sending a crafted SNMP request. **CVE ID : CVE-2020-14936**	N/A	O-CON-CONT-070920/507
Out-of-bounds Write	18-Aug-20	6.4	Memory access out of buffer boundaries issues was	N/A	O-CON-CONT-070920/508

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
			discovered in Contiki-NG 4.4 through 4.5, in the SNMP BER encoder/decoder. The length of provided input/output buffers is insufficiently verified during the encoding and decoding of data. This may lead to out-of-bounds buffer read or write access in BER decoding and encoding functions. **CVE ID : CVE-2020-14937**		
Debian					
debian_linux					
Untrusted Search Path	24-Aug-20	4.4	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension. This affects PostgreSQL versions before 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23. **CVE ID : CVE-2020-14350**	N/A	O-DEB-DEBI-070920/509
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Aug-20	4.3	Icinga Icinga Web2 2.0.0 through 2.6.4, 2.7.4 and 2.8.2 has a Directory Traversal vulnerability which allows an attacker to access arbitrary files that are readable by the process running Icinga Web 2. This issue is fixed in Icinga Web 2 in v2.6.4, v2.7.4 and v2.8.2.	https://icinga.com/2020/08/19/icinga-web-security-release-v2-6-4-v2-7-4-and-v2-8-2/	O-DEB-DEBI-070920/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-24368		
Improper Handling of Exceptional Conditions	21-Aug-20	4	A user authorized to perform database queries may cause denial of service by issuing specially crafted queries, which violate an invariant in the query subsystem's support for geoNear. This issue affects: MongoDB Inc. MongoDB Server v4.5 versions prior to 4.5.1; v4.4 versions prior to 4.4.0-rc7; v4.2 versions prior to 4.2.8; v4.0 versions prior to 4.0.19. **CVE ID : CVE-2020-7923**	N/A	O-DEB-DEBI-070920/511
Fedoraproject					
fedora					
Reachable Assertion	21-Aug-20	4	In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit. Alternately, an off-path attacker would have to correctly guess when a TSIG-signed request was sent, along with other characteristics of the packet and message, and spoof a truncated response to trigger an assertion failure, causing	https://kb.isc.org/docs/cve-2020-8622, https://security.netapp.com/advisory/ntap-20200827-0003/, https://www.synology.com/security/advisory/Synology_SA_20_19	O-FED-FEDO-070920/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the server to exit. **CVE ID : CVE-2020-8622**		
Improper Privilege Management	21-Aug-20	4.3	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND that was built with "--enable-native-pkcs11" * be signing one or more zones with an RSA key * be able to receive queries from a possible attacker **CVE ID : CVE-2020-8623**	https://kb.isc.org/docs/cve-2020-8623, https://security.netapp.com/advisory/ntap-20200827-0003/, https://www.synology.com/security/advisory/Synology_SA_20_19	O-FED-FEDO-070920/513
Improper Privilege Management	21-Aug-20	4	In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could abuse these unintended additional privileges to update other contents of the zone. **CVE ID : CVE-2020-8624**	https://kb.isc.org/docs/cve-2020-8624, https://security.netapp.com/advisory/ntap-20200827-0003/, https://www.synology.com/security/advisory/Synology_SA_20_19	O-FED-FEDO-070920/514
Huawei					
e6878-370_firmware					
Incorrect Authorizatio	17-Aug-20	6.8	Huawei 5G Mobile WiFi E6878-370 with versions of	N/A	O-HUA-E687-070920/515

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
n			10.0.3.1(H563SP1C00),10.0.3.1(H563SP21C233) have an improper authorization vulnerability. The device does not restrict certain data received from WAN port. Successful exploit could allow an attacker at WAN side to manage certain service of the device. **CVE ID : CVE-2020-9241**		
taurus-al00b_firmware					
Use After Free	17-Aug-20	4.6	Huawei smartphone Taurus-AL00B with versions earlier than 10.1.0.126(C00E125R5P3) have a user after free vulnerability. A module is lack of lock protection. Attackers can exploit this vulnerability by launching specific request. This could compromise normal service of the affected device. **CVE ID : CVE-2020-9237**	N/A	O-HUA-TAUR-070920/516
p30_pro_firmware					
Integer Overflow or Wraparound	21-Aug-20	2.1	HUAWEI P30 Pro smartphone with Versions earlier than 10.1.0.160(C00E160R2P8) has an integer overflow vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this vulnerability by send malicious message to cause integer overflow. This can compromise normal service.	N/A	O-HUA-P30_-070920/517

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-2020-9095		
Out-of-bounds Read	21-Aug-20	2.1	HUAWEI P30 Pro smartphones with Versions earlier than 10.1.0.160(C00E160R2P8) have an out of bound read vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this vulnerability by send malicious message to cause out-of-bound read. This can compromise normal service. **CVE ID : CVE-2020-9096**	N/A	O-HUA-P30_-070920/518
p30_firmware					
Improper Release of Memory Before Removing Last Reference	21-Aug-20	3.3	HUAWEI P30 smartphones with Versions earlier than 10.1.0.123(C431E22R2P5),Versions earlier than 10.1.0.123(C432E22R2P5),Versions earlier than 10.1.0.126(C10E7R5P1),Versions earlier than 10.1.0.126(C185E4R7P1),Versions earlier than 10.1.0.126(C461E7R3P1),Versions earlier than 10.1.0.126(C605E19R1P3),Versions earlier than 10.1.0.126(C636E7R3P4),Versions earlier than 10.1.0.128(C635E3R2P4),Versions earlier than 10.1.0.160(C00E160R2P11),Versions earlier than 10.1.0.160(C01E160R2P11) have a denial of service vulnerability. In specific	N/A	O-HUA-P30_-070920/519

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
			scenario, due to the improper resource management and memory leak of some feature, the attacker could exploit this vulnerability to cause the device reset. **CVE ID : CVE-2020-9104**		
mate_20_firmware					
N/A	17-Aug-20	2.1	HUAWEI Mate 20 smartphones with 9.0.0.205(C00E205R2P1) have a logic error vulnerability. In a special scenario, the system does not properly process. As a result, attackers can perform a series of operations to successfully establish P2P connections that are rejected by the peer end. As a result, the availability of the device is affected. **CVE ID : CVE-2020-9103**	N/A	O-HUA-MATE-070920/520
IBM					
flashsystem_v5000_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	O-IBM-FLAS-070920/521
flashsystem_v7200_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and	https://www.ibm.com/support/pages/node/6	O-IBM-FLAS-070920/522

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
			perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	260199	
flashsystem_v9000_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	O-IBM-FLAS-070920/523
flashsystem_v9100_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	O-IBM-FLAS-070920/524
flashsystem_v9200_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	O-IBM-FLAS-070920/525
san_volume_controller_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should	https://www.ibm.com/support/pages/node/6260199	O-IBM-SAN_-070920/526

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
			not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**		
storwize_v5000_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	O-IBM-STOR-070920/527
storwize_v5000e_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	O-IBM-STOR-070920/528
storwize_v5100_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	O-IBM-STOR-070920/529
storwize_v7000_firmware					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-	https://www.ibm.com/support/pages/node/6260199	O-IBM-STOR-070920/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Force ID: 186678. **CVE ID : CVE-2020-4686**		
AIX					
Improper Input Validation	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 is vulnerable to improper input validation. A malicious administrator could bypass the user interface and send requests to the IBM Content Navigator server with illegal characters that could be stored in the IBM Content Navigator database. IBM X-Force ID: 183316. **CVE ID : CVE-2020-4548**	https://www.ibm.com/support/pages/node/6262411	O-IBM-AIX-070920/531
Information Exposure	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 could allow an authenticated user to view cached content of another user that they should not have access to. IBM X-Force ID: 186679. **CVE ID : CVE-2020-4687**	https://www.ibm.com/support/pages/node/6262423	O-IBM-AIX-070920/532
Linux					
linux_kernel					
Improper Input Validation	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 is vulnerable to improper input validation. A malicious administrator could bypass the user interface and send requests to the IBM Content Navigator server with illegal characters that could be stored in the IBM Content Navigator database. IBM X-Force ID: 183316. **CVE ID : CVE-2020-4548**	https://www.ibm.com/support/pages/node/6262411	O-LIN-LINU-070920/533

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
NULL Pointer Dereference	19-Aug-20	7.2	A flaw null pointer dereference in the Linux kernel cgroupv2 subsystem in versions before 5.7.10 was found in the way when reboot the system. A local user could use this flaw to crash the system or escalate their privileges on the system. **CVE ID : CVE-2020-14356**	N/A	O-LIN-LINU-070920/534
Incorrect Default Permissions	19-Aug-20	4.6	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered. **CVE ID : CVE-2020-24394**	N/A	O-LIN-LINU-070920/535
Cross-Site Request Forgery (CSRF)	24-Aug-20	4.3	IBM Security Guardium Insights 2.0.1 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: 174406. **CVE ID : CVE-2020-4170**	https://www.ibm.com/support/pages/node/6320055	O-LIN-LINU-070920/536
Improper Input Validation	24-Aug-20	2.1	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment or upgrade pertaining to xcat services. IBM X-Force ID: 179163. **CVE ID : CVE-2020-4382**	https://www.ibm.com/support/pages/node/6320001	O-LIN-LINU-070920/537

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 Input Validation	24-Aug-20	4	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment while configuring some of the network services. IBM X-Force ID: 179165. **CVE ID : CVE-2020-4383**	https://www.ibm.com/support/pages/node/6320003	O-LIN-LINU-070920/538
Insufficiently Protected Credentials	24-Aug-20	2.1	IBM Security Guardium Insights 2.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 184747. **CVE ID : CVE-2020-4593**	https://www.ibm.com/support/pages/node/6320067	O-LIN-LINU-070920/539
URL Redirection to Untrusted Site ('Open Redirect')	24-Aug-20	5.8	IBM Security Guardium Insights 2.0.1 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 184823. **CVE ID : CVE-2020-4598**	https://www.ibm.com/support/pages/node/6320061	O-LIN-LINU-070920/540
Information Exposure	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 could allow an authenticated user to view cached content of another	https://www.ibm.com/support/pages/node/6	O-LIN-LINU-070920/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user that they should not have access to. IBM X-Force ID: 186679. **CVE ID : CVE-2020-4687**	262423	
Microsoft					
windows					
Improper Input Validation	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 is vulnerable to improper input validation. A malicious administrator could bypass the user interface and send requests to the IBM Content Navigator server with illegal characters that could be stored in the IBM Content Navigator database. IBM X-Force ID: 183316. **CVE ID : CVE-2020-4548**	https://www.ibm.com/support/pages/node/6262411	O-MIC-WIND-070920/542
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9721**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/543
Use After Free	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9722**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/544

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
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9723**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/545
Improper Privilege Management	19-Aug-20	6.8	Adobe Lightroom versions 9.2.0.10 and earlier have an insecure library loading vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9724**	https://helpx.adobe.com/security/products/lightroom/apsb20-51.html	O-MIC-WIND-070920/546
Out-of-bounds Write	20-Aug-20	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. 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 TIF 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 context of the current process. Was ZDI-CAN-10764. **CVE ID : CVE-2020-15629**	N/A	O-MIC-WIND-070920/547

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
Out-of-bounds Read	20-Aug-20	6.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. 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 PNG 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-10977. **CVE ID : CVE-2020-15630**	N/A	O-MIC-WIND-070920/548
Use After Free	20-Aug-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. 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 SetLocalDescription method. By performing actions in JavaScript, an attacker can cause a pointer to be reused after it has been freed. An attacker can leverage this in	N/A	O-MIC-WIND-070920/549

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
			conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10972. **CVE ID : CVE-2020-15637**		
Access of Resource Using Incompatible Type ('Type Confusion')	20-Aug-20	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.2.29539. 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 NodeProperties::InferReceiverMapsUnsafe method. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10950. **CVE ID : CVE-2020-15638**	N/A	O-MIC-WIND-070920/550
Information Exposure	20-Aug-20	4	IBM Content Navigator 3.0.7 and 3.0.8 could allow an authenticated user to view cached content of another user that they should not have access to. IBM X-Force ID: 186679. **CVE ID : CVE-2020-4687**	https://www.ibm.com/support/pages/node/6262423	O-MIC-WIND-070920/551
Stack-based Buffer	20-Aug-20	6.8	This vulnerability allows remote attackers to execute	N/A	O-MIC-WIND-070920/552

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
Overflow			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 TIF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9881. **CVE ID : CVE-2020-8869**		
Out-of-bounds Read	20-Aug-20	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 TIF files from the GetTIFPalette method. 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	N/A	O-MIC-WIND-070920/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process. Was ZDI-CAN-9931. **CVE ID : CVE-2020-8870**		
Out-of-bounds Write	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9693**	N/A	O-MIC-WIND-070920/554
Out-of-bounds Write	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9694**	N/A	O-MIC-WIND-070920/555
Incorrect Authorization	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9696**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/556
Information Exposure	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a disclosure of sensitive data vulnerability.	https://helpx.adobe.com/security/products/acrobat/apsb20-	O-MIC-WIND-070920/557

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
			Successful exploitation could lead to memory leak. **CVE ID : CVE-2020-9697**	48.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9698**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/558
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9699**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9700**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/560
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error	https://helpx.adobe.com/security/products/acrobat/apsb20-	O-MIC-WIND-070920/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9701**	48.html	
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9702**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/562
Uncontrolled Resource Consumption	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9703**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/563
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9704**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/564
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002,	https://helpx.adobe.com/security	O-MIC-WIND-070920/565

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
			2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9705**	/products/acrobat/apsb20-48.html	
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9706**	N/A	O-MIC-WIND-070920/566
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9707**	N/A	O-MIC-WIND-070920/567
Out-of-bounds Read	19-Aug-20	4.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9710**	N/A	O-MIC-WIND-070920/568
Incorrect Authorizatio	19-Aug-20	7.1	Adobe Acrobat and Reader versions 2020.009.20074 and	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9712**		070920/569
Improper Privilege Management	19-Aug-20	6.8	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation . **CVE ID : CVE-2020-9714**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/570
Use After Free	19-Aug-20	9.3	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9715**	N/A	O-MIC-WIND-070920/571
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9716**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/572

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
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9717**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/573
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9718**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/574
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9719**	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/575
Out-of-bounds Read	19-Aug-20	5	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html	O-MIC-WIND-070920/576

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-2020-9720		
windows_10					
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists on ARM implementations that use speculative execution in control flow via a side-channel analysis, aka &quot;straight-line speculation, aka 'Windows ARM Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1459**	N/A	O-MIC-WIND-070920/577
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1512**	N/A	O-MIC-WIND-070920/578
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**	N/A	O-MIC-WIND-070920/579
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this	N/A	O-MIC-WIND-070920/580

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
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**	N/A	O-MIC-WIND-070920/581
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**	N/A	O-MIC-WIND-070920/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1538. **CVE ID : CVE-2020-1519**	N/A	O-MIC-WIND-070920/583
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1520**	N/A	O-MIC-WIND-070920/584
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Runtime Elevation of	N/A	O-MIC-WIND-070920/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1522. **CVE ID : CVE-2020-1521**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1521. **CVE ID : CVE-2020-1522**	N/A	O-MIC-WIND-070920/586
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Shell Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Shell Components Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1524**	N/A	O-MIC-WIND-070920/587
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-	N/A	O-MIC-WIND-070920/588

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
			1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1554. **CVE ID : CVE-2020-1525**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Network Connection Broker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Connection Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1526**	N/A	O-MIC-WIND-070920/589
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Custom Protocol Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Custom Protocol Engine Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1527**	N/A	O-MIC-WIND-070920/590
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Radio Manager API improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Radio Manager API Elevation of	N/A	O-MIC-WIND-070920/591

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
			Privilege Vulnerability'. **CVE ID : CVE-2020-1528**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547. **CVE ID : CVE-2020-1551**	N/A	O-MIC-WIND-070920/592
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/593
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1553**	N/A	O-MIC-WIND-070920/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	O-MIC-WIND-070920/595
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/596
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**	N/A	O-MIC-WIND-070920/597
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1378. **CVE ID : CVE-2020-1377**	N/A	O-MIC-WIND-070920/598
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation	N/A	O-MIC-WIND-070920/599

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
			of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/600
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**	N/A	O-MIC-WIND-070920/601
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**	N/A	O-MIC-WIND-070920/602
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in	N/A	O-MIC-WIND-070920/603

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
			memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1486, CVE-2020-1566. **CVE ID : CVE-2020-1417**		
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/604
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1467**	N/A	O-MIC-WIND-070920/605
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**	N/A	O-MIC-WIND-070920/606
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	6.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code	N/A	O-MIC-WIND-070920/607

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
Buffer			Execution Vulnerability'. This CVE ID is unique from CVE-2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**	N/A	O-MIC-WIND-070920/608
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/609
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	O-MIC-WIND-070920/610
Improper Restriction of Operations within the Bounds of a	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media	N/A	O-MIC-WIND-070920/611

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
Memory Buffer			Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**	N/A	O-MIC-WIND-070920/612
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1479**	N/A	O-MIC-WIND-070920/613
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1529. **CVE ID : CVE-2020-1480**	N/A	O-MIC-WIND-070920/614
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders	N/A	O-MIC-WIND-070920/615

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
Management			Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**	N/A	O-MIC-WIND-070920/616
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**	N/A	O-MIC-WIND-070920/617
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-070920/618

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-2020-1487		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1488**	N/A	O-MIC-WIND-070920/619
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**	N/A	O-MIC-WIND-070920/620
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege	N/A	O-MIC-WIND-070920/621

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
			Vulnerability'. **CVE ID : CVE-2020-1490**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1492**	N/A	O-MIC-WIND-070920/622
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/623
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1510**	N/A	O-MIC-WIND-070920/624
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file	N/A	O-MIC-WIND-070920/625

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
			operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1511**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489. **CVE ID : CVE-2020-1513**	N/A	O-MIC-WIND-070920/626
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1480. **CVE ID : CVE-2020-1529**	N/A	O-MIC-WIND-070920/627
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-070920/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1531**	N/A	O-MIC-WIND-070920/629
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1556. **CVE ID : CVE-2020-1533**	N/A	O-MIC-WIND-070920/630
Improper Privilege Management	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1534**	N/A	O-MIC-WIND-070920/631
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine	N/A	O-MIC-WIND-070920/632

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
Management			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1535**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1536**	N/A	O-MIC-WIND-070920/633
Improper Restriction of Operations within the Bounds of a	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations, aka 'Windows	N/A	O-MIC-WIND-070920/634

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
Memory Buffer			Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**	N/A	O-MIC-WIND-070920/635
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1539**	N/A	O-MIC-WIND-070920/636
Improper	17-Aug-20	4.6	An elevation of privilege	N/A	O-MIC-WIND-

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
Privilege Management			vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1540**		070920/637
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1541**	N/A	O-MIC-WIND-070920/638
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine	N/A	O-MIC-WIND-070920/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1542**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1543**	N/A	O-MIC-WIND-070920/640
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this	N/A	O-MIC-WIND-070920/641

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
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1544**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1545**	N/A	O-MIC-WIND-070920/642
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-070920/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1546**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1551. **CVE ID : CVE-2020-1547**	N/A	O-MIC-WIND-070920/644
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows WaasMedic Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows	N/A	O-MIC-WIND-070920/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WaasMedic Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1548**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CDP User Components Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1550. **CVE ID : CVE-2020-1549**	N/A	O-MIC-WIND-070920/646
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CDP User Components Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1549. **CVE ID : CVE-2020-1550**	N/A	O-MIC-WIND-070920/647
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'.	N/A	O-MIC-WIND-070920/648

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
			This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **CVE ID : CVE-2020-1554**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1570. **CVE ID : CVE-2020-1555**	N/A	O-MIC-WIND-070920/649
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1533. **CVE ID : CVE-2020-1556**	N/A	O-MIC-WIND-070920/650
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1557**	N/A	O-MIC-WIND-070920/651
Improper Restriction of	17-Aug-20	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-

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
Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**		070920/652
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.9	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1574, CVE-2020-1585. **CVE ID : CVE-2020-1560**	N/A	O-MIC-WIND-070920/653
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1562. **CVE ID : CVE-2020-1561**	N/A	O-MIC-WIND-070920/654
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1561.	N/A	O-MIC-WIND-070920/655

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
			CVE ID : CVE-2020-1562		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1558. **CVE ID : CVE-2020-1564**	N/A	O-MIC-WIND-070920/656
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1565**	N/A	O-MIC-WIND-070920/657
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1486. **CVE ID : CVE-2020-1566**	N/A	O-MIC-WIND-070920/658
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An	N/A	O-MIC-WIND-070920/659

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
			attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1568**	N/A	O-MIC-WIND-070920/660
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1569**	N/A	O-MIC-WIND-070920/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**	N/A	O-MIC-WIND-070920/662
Incorrect Default Permissions	17-Aug-20	7.2	An elevation of privilege vulnerability exists in Windows Setup in the way it handles permissions.A locally authenticated attacker could run arbitrary code with elevated system privileges,	N/A	O-MIC-WIND-070920/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Windows Setup Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1571**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.9	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1560, CVE-2020-1585. **CVE ID : CVE-2020-1574**	N/A	O-MIC-WIND-070920/664
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1577**	N/A	O-MIC-WIND-070920/665
Information Exposure	17-Aug-20	1.9	An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1578**	N/A	O-MIC-WIND-070920/666
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-070920/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/668
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1560, CVE-2020-1574. **CVE ID : CVE-2020-1585**	N/A	O-MIC-WIND-070920/669
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-070920/670

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
			CVE ID : CVE-2020-1587		
windows_7					
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**	N/A	O-MIC-WIND-070920/671
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**	N/A	O-MIC-WIND-070920/672
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management	N/A	O-MIC-WIND-070920/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**	N/A	O-MIC-WIND-070920/674
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1538. **CVE ID : CVE-2020-1519**	N/A	O-MIC-WIND-070920/675
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	7.2	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the	N/A	O-MIC-WIND-070920/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1520**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Network Connection Broker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Connection Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1526**	N/A	O-MIC-WIND-070920/677
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-	N/A	O-MIC-WIND-070920/678

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
			1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547. **CVE ID : CVE-2020-1551**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/679
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	O-MIC-WIND-070920/680
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/681
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**	N/A	O-MIC-WIND-070920/682
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API	N/A	O-MIC-WIND-070920/683

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
			improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1378. **CVE ID : CVE-2020-1377**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**	N/A	O-MIC-WIND-070920/684
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/685
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570.	N/A	O-MIC-WIND-070920/686

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-2020-1380		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**	N/A	O-MIC-WIND-070920/687
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/688
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1467**	N/A	O-MIC-WIND-070920/689
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**	N/A	O-MIC-WIND-070920/690
Improper Restriction of	17-Aug-20	6.8	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-070920/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**	N/A	O-MIC-WIND-070920/692
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/693
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	O-MIC-WIND-070920/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**	N/A	O-MIC-WIND-070920/695
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**	N/A	O-MIC-WIND-070920/696
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**	N/A	O-MIC-WIND-070920/697
Information	17-Aug-20	2.1	An information disclosure	N/A	O-MIC-WIND-

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			vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**		070920/698
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**	N/A	O-MIC-WIND-070920/699
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**	N/A	O-MIC-WIND-070920/700
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory	N/A	O-MIC-WIND-070920/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1492**		
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/702
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489. **CVE ID : CVE-2020-1513**	N/A	O-MIC-WIND-070920/703
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-070920/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1480. **CVE ID : CVE-2020-1529**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**	N/A	O-MIC-WIND-070920/705
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1531**	N/A	O-MIC-WIND-070920/706
Improper Privilege Management	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1534**	N/A	O-MIC-WIND-070920/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1535**	N/A	O-MIC-WIND-070920/708
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1536**	N/A	O-MIC-WIND-070920/709
Improper Restriction of	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-070920/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Windows Remote Access improperly handles file operations, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**	N/A	O-MIC-WIND-070920/711
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	N/A	O-MIC-WIND-070920/712

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-2020-1539		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1540**	N/A	O-MIC-WIND-070920/713
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1541**	N/A	O-MIC-WIND-070920/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1542**	N/A	O-MIC-WIND-070920/715
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1543**	N/A	O-MIC-WIND-070920/716
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-070920/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1544**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1545**	N/A	O-MIC-WIND-070920/718
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles	N/A	O-MIC-WIND-070920/719

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
			memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1546**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1551. **CVE ID : CVE-2020-1547**	N/A	O-MIC-WIND-070920/720
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory	N/A	O-MIC-WIND-070920/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **CVE ID : CVE-2020-1554**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1557**	N/A	O-MIC-WIND-070920/722
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**	N/A	O-MIC-WIND-070920/723
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1561. **CVE ID : CVE-2020-1562**	N/A	O-MIC-WIND-070920/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1558. **CVE ID : CVE-2020-1564**	N/A	O-MIC-WIND-070920/725
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1565**	N/A	O-MIC-WIND-070920/726
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**	N/A	O-MIC-WIND-070920/727
Improper Restriction of Operations within the Bounds of a	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka	N/A	O-MIC-WIND-070920/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**		
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1577**	N/A	O-MIC-WIND-070920/729
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**	N/A	O-MIC-WIND-070920/730
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/731
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock	N/A	O-MIC-WIND-070920/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1587**		
windows_8.1					
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**	N/A	O-MIC-WIND-070920/733
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**	N/A	O-MIC-WIND-070920/734
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-070920/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**	N/A	O-MIC-WIND-070920/736
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-070920/737

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
			2020-1538. **CVE ID : CVE-2020-1519**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1520**	N/A	O-MIC-WIND-070920/738
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Network Connection Broker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Connection Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1526**	N/A	O-MIC-WIND-070920/739
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-070920/740

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
			execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547. **CVE ID : CVE-2020-1551**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/741
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	O-MIC-WIND-070920/742
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/743
Improper Restriction of	17-Aug-20	9.3	A remote code execution vulnerability exists when	N/A	O-MIC-WIND-

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
Operations within the Bounds of a Memory Buffer			Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**		070920/744
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1378. **CVE ID : CVE-2020-1377**	N/A	O-MIC-WIND-070920/745
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**	N/A	O-MIC-WIND-070920/746
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/747
Improper Restriction of	17-Aug-20	7.6	A remote code execution vulnerability exists in the way	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**		070920/748
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**	N/A	O-MIC-WIND-070920/749
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/750
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1467**	N/A	O-MIC-WIND-070920/751
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work	N/A	O-MIC-WIND-070920/752

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
			Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**	N/A	O-MIC-WIND-070920/753
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**	N/A	O-MIC-WIND-070920/754
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/755
Improper Privilege	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web	N/A	O-MIC-WIND-070920/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**	N/A	O-MIC-WIND-070920/757
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**	N/A	O-MIC-WIND-070920/758
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work	N/A	O-MIC-WIND-070920/759

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
			Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**	N/A	O-MIC-WIND-070920/760
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**	N/A	O-MIC-WIND-070920/761
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1487**	N/A	O-MIC-WIND-070920/762
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege	N/A	O-MIC-WIND-070920/763

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
			management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1488**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**	N/A	O-MIC-WIND-070920/764
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554.	N/A	O-MIC-WIND-070920/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1492		
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/766
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489. **CVE ID : CVE-2020-1513**	N/A	O-MIC-WIND-070920/767
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1480. **CVE ID : CVE-2020-1529**	N/A	O-MIC-WIND-070920/768
Improper Restriction of Operations	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access	N/A	O-MIC-WIND-070920/769

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			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1531**	N/A	O-MIC-WIND-070920/770
Improper Privilege Management	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1534**	N/A	O-MIC-WIND-070920/771
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this	N/A	O-MIC-WIND-070920/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1535**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1536**	N/A	O-MIC-WIND-070920/773
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-070920/774

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 is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**	N/A	O-MIC-WIND-070920/775
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1539**	N/A	O-MIC-WIND-070920/776
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine	N/A	O-MIC-WIND-070920/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1540**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1541**	N/A	O-MIC-WIND-070920/778
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this	N/A	O-MIC-WIND-070920/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1542**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1543**	N/A	O-MIC-WIND-070920/780
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-070920/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1544**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1545**	N/A	O-MIC-WIND-070920/782
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup	N/A	O-MIC-WIND-070920/783

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
			Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1546**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1551. **CVE ID : CVE-2020-1547**	N/A	O-MIC-WIND-070920/784
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525.	N/A	O-MIC-WIND-070920/785

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-2020-1554		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1557**	N/A	O-MIC-WIND-070920/786
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**	N/A	O-MIC-WIND-070920/787
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1561. **CVE ID : CVE-2020-1562**	N/A	O-MIC-WIND-070920/788
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code	N/A	O-MIC-WIND-070920/789

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
Buffer			Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1558. **CVE ID : CVE-2020-1564**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1565**	N/A	O-MIC-WIND-070920/790
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**	N/A	O-MIC-WIND-070920/791
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**	N/A	O-MIC-WIND-070920/792

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
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1577**	N/A	O-MIC-WIND-070920/793
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**	N/A	O-MIC-WIND-070920/794
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/795
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows	N/A	O-MIC-WIND-070920/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1587**		
windows_rt_8.1					
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**	N/A	O-MIC-WIND-070920/797
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**	N/A	O-MIC-WIND-070920/798
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-070920/799

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
			execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**	N/A	O-MIC-WIND-070920/800
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1538. **CVE ID : CVE-2020-1519**	N/A	O-MIC-WIND-070920/801
Improper Restriction of Operations	17-Aug-20	7.2	A remote code execution vulnerability exists when the Windows Font Driver Host	N/A	O-MIC-WIND-070920/802

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			improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1520**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Network Connection Broker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Connection Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1526**	N/A	O-MIC-WIND-070920/803
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-	N/A	O-MIC-WIND-070920/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547. **CVE ID : CVE-2020-1551**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/805
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/806
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**	N/A	O-MIC-WIND-070920/807
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-070920/808

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-2020-1378. **CVE ID : CVE-2020-1377**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**	N/A	O-MIC-WIND-070920/809
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/810
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**	N/A	O-MIC-WIND-070920/811
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka	N/A	O-MIC-WIND-070920/812

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
			'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**		
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/813
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1467**	N/A	O-MIC-WIND-070920/814
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**	N/A	O-MIC-WIND-070920/815
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-070920/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**	N/A	O-MIC-WIND-070920/817
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/818
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	O-MIC-WIND-070920/819
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'.	N/A	O-MIC-WIND-070920/820

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
Buffer			This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**	N/A	O-MIC-WIND-070920/821
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**	N/A	O-MIC-WIND-070920/822
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure	N/A	O-MIC-WIND-070920/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**	N/A	O-MIC-WIND-070920/824
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1487**	N/A	O-MIC-WIND-070920/825
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of	N/A	O-MIC-WIND-070920/826

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
			Privilege Vulnerability'. **CVE ID : CVE-2020-1488**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**	N/A	O-MIC-WIND-070920/827
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1492**	N/A	O-MIC-WIND-070920/828
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489. **CVE ID : CVE-2020-1513**	N/A	O-MIC-WIND-070920/830
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1480. **CVE ID : CVE-2020-1529**	N/A	O-MIC-WIND-070920/831
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**	N/A	O-MIC-WIND-070920/832
Improper Restriction of Operations	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control	N/A	O-MIC-WIND-070920/833

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			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1531**		
Improper Privilege Management	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1534**	N/A	O-MIC-WIND-070920/834
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	N/A	O-MIC-WIND-070920/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1535		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1536**	N/A	O-MIC-WIND-070920/836
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**	N/A	O-MIC-WIND-070920/837
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of	N/A	O-MIC-WIND-070920/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1539**	N/A	O-MIC-WIND-070920/839
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-	N/A	O-MIC-WIND-070920/840

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
			2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1540**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1541**	N/A	O-MIC-WIND-070920/841
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551.	N/A	O-MIC-WIND-070920/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1542		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1543**	N/A	O-MIC-WIND-070920/843
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1545, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1544**	N/A	O-MIC-WIND-070920/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1546, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1545**	N/A	O-MIC-WIND-070920/845
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1547, CVE-2020-1551. **CVE ID : CVE-2020-1546**	N/A	O-MIC-WIND-070920/846
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-070920/847

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
Management			Windows Backup Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Engine Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1535, CVE-2020-1536, CVE-2020-1539, CVE-2020-1540, CVE-2020-1541, CVE-2020-1542, CVE-2020-1543, CVE-2020-1544, CVE-2020-1545, CVE-2020-1546, CVE-2020-1551. **CVE ID : CVE-2020-1547**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **CVE ID : CVE-2020-1554**	N/A	O-MIC-WIND-070920/848
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1558, CVE-2020-1564.	N/A	O-MIC-WIND-070920/849

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-2020-1557		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**	N/A	O-MIC-WIND-070920/850
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1561. **CVE ID : CVE-2020-1562**	N/A	O-MIC-WIND-070920/851
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1558. **CVE ID : CVE-2020-1564**	N/A	O-MIC-WIND-070920/852
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this	N/A	O-MIC-WIND-070920/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1565**		
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**	N/A	O-MIC-WIND-070920/854
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**	N/A	O-MIC-WIND-070920/855
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1577**	N/A	O-MIC-WIND-070920/856
Improper Privilege	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery	N/A	O-MIC-WIND-070920/857

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
Management			SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/858
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1587**	N/A	O-MIC-WIND-070920/859
windows_server_2008					
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-070920/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**	N/A	O-MIC-WIND-070920/861
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**	N/A	O-MIC-WIND-070920/862
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management	N/A	O-MIC-WIND-070920/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1538. **CVE ID : CVE-2020-1519**	N/A	O-MIC-WIND-070920/864
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-070920/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1520		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/866
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	O-MIC-WIND-070920/867
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/868
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**	N/A	O-MIC-WIND-070920/869
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka	N/A	O-MIC-WIND-070920/870

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
			'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1378. **CVE ID : CVE-2020-1377**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**	N/A	O-MIC-WIND-070920/871
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/872
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**	N/A	O-MIC-WIND-070920/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**	N/A	O-MIC-WIND-070920/874
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/875
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1467**	N/A	O-MIC-WIND-070920/876
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**	N/A	O-MIC-WIND-070920/877
Improper Privilege Management	17-Aug-20	9.3	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure	N/A	O-MIC-WIND-070920/878

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
			channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1472**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**	N/A	O-MIC-WIND-070920/879
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**	N/A	O-MIC-WIND-070920/880
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	O-MIC-WIND-070920/882
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**	N/A	O-MIC-WIND-070920/883
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**	N/A	O-MIC-WIND-070920/884
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-070920/885

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
			would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**	N/A	O-MIC-WIND-070920/886
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**	N/A	O-MIC-WIND-070920/887
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege	N/A	O-MIC-WIND-070920/888

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
			Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1492**	N/A	O-MIC-WIND-070920/889
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/890
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489.	N/A	O-MIC-WIND-070920/891

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-2020-1513		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1480. **CVE ID : CVE-2020-1529**	N/A	O-MIC-WIND-070920/892
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**	N/A	O-MIC-WIND-070920/893
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1531**	N/A	O-MIC-WIND-070920/894
Improper Privilege Management	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Backup Service	N/A	O-MIC-WIND-070920/895

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
			improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**	N/A	O-MIC-WIND-070920/896
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**	N/A	O-MIC-WIND-070920/897
Improper Restriction of Operations within the Bounds of a Memory	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory	N/A	O-MIC-WIND-070920/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **CVE ID : CVE-2020-1554**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1557**	N/A	O-MIC-WIND-070920/899
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**	N/A	O-MIC-WIND-070920/900
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1561. **CVE ID : CVE-2020-1562**	N/A	O-MIC-WIND-070920/901

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 Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1558. **CVE ID : CVE-2020-1564**	N/A	O-MIC-WIND-070920/902
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**	N/A	O-MIC-WIND-070920/903
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**	N/A	O-MIC-WIND-070920/904
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-070920/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1577		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**	N/A	O-MIC-WIND-070920/906
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/907
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1587**	N/A	O-MIC-WIND-070920/908
windows_server_2012					
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**		070920/909
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**	N/A	O-MIC-WIND-070920/910
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**	N/A	O-MIC-WIND-070920/911

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	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**	N/A	O-MIC-WIND-070920/912
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1538. **CVE ID : CVE-2020-1519**	N/A	O-MIC-WIND-070920/913
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows	N/A	O-MIC-WIND-070920/914

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
			Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1520**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/915
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	O-MIC-WIND-070920/916
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/917
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**	N/A	O-MIC-WIND-070920/918
Improper	17-Aug-20	7.2	An elevation of privilege	N/A	O-MIC-WIND-

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
Privilege Management			vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1378. **CVE ID : CVE-2020-1377**		070920/919
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**	N/A	O-MIC-WIND-070920/920
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/921
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-070920/922

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-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**	N/A	O-MIC-WIND-070920/923
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/924
Improper Input Validation	17-Aug-20	5	A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability'. **CVE ID : CVE-2020-1466**	N/A	O-MIC-WIND-070920/925
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1467**	N/A	O-MIC-WIND-070920/926
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-070920/927

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
Management			Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**		
Improper Privilege Management	17-Aug-20	9.3	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1472**	N/A	O-MIC-WIND-070920/928
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**	N/A	O-MIC-WIND-070920/929
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its	N/A	O-MIC-WIND-070920/930

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
			memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/931
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	O-MIC-WIND-070920/932
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**	N/A	O-MIC-WIND-070920/933
Improper Restriction of Operations	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation	N/A	O-MIC-WIND-070920/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**	N/A	O-MIC-WIND-070920/935
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**	N/A	O-MIC-WIND-070920/936
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows	N/A	O-MIC-WIND-070920/937

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
			Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**		
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1487**	N/A	O-MIC-WIND-070920/938
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1488**	N/A	O-MIC-WIND-070920/939
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-070920/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1492**	N/A	O-MIC-WIND-070920/941
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/942
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim	N/A	O-MIC-WIND-070920/943

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
			system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489. **CVE ID : CVE-2020-1513**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1480. **CVE ID : CVE-2020-1529**	N/A	O-MIC-WIND-070920/944
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**	N/A	O-MIC-WIND-070920/945
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-070920/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1531		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**	N/A	O-MIC-WIND-070920/947
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**	N/A	O-MIC-WIND-070920/948
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **CVE ID : CVE-2020-1554**	N/A	O-MIC-WIND-070920/949
Improper Restriction of	17-Aug-20	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-070920/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1557**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**	N/A	O-MIC-WIND-070920/951
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1561. **CVE ID : CVE-2020-1562**	N/A	O-MIC-WIND-070920/952
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557,	N/A	O-MIC-WIND-070920/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1558. **CVE ID : CVE-2020-1564**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1565**	N/A	O-MIC-WIND-070920/954
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**	N/A	O-MIC-WIND-070920/955
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**	N/A	O-MIC-WIND-070920/956
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly	N/A	O-MIC-WIND-070920/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1577**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**	N/A	O-MIC-WIND-070920/958
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/959
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-070920/960

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-2020-1587		
windows_server_2016					
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1512**	N/A	O-MIC-WIND-070920/961
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**	N/A	O-MIC-WIND-070920/962
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**	N/A	O-MIC-WIND-070920/963
Improper Privilege	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-

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
Management			Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**		070920/964
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**	N/A	O-MIC-WIND-070920/965
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-070920/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1538. **CVE ID : CVE-2020-1519**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1520**	N/A	O-MIC-WIND-070920/967
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1522. **CVE ID : CVE-2020-1521**	N/A	O-MIC-WIND-070920/968
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-070920/969

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
			execution on the victim system, aka 'Windows Speech Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1521. **CVE ID : CVE-2020-1522**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Shell Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Shell Components Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1524**	N/A	O-MIC-WIND-070920/970
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1554. **CVE ID : CVE-2020-1525**	N/A	O-MIC-WIND-070920/971
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Network Connection Broker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-070920/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows Network Connection Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1526**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Custom Protocol Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Custom Protocol Engine Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1527**	N/A	O-MIC-WIND-070920/973
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Radio Manager API improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Radio Manager API Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1528**	N/A	O-MIC-WIND-070920/974
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/975

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 Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1553**	N/A	O-MIC-WIND-070920/976
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	O-MIC-WIND-070920/977
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/978
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**	N/A	O-MIC-WIND-070920/979
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-070920/980

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
			CVE-2020-1378. **CVE ID : CVE-2020-1377**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**	N/A	O-MIC-WIND-070920/981
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/982
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**	N/A	O-MIC-WIND-070920/983
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka	N/A	O-MIC-WIND-070920/984

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
			'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1486, CVE-2020-1566. **CVE ID : CVE-2020-1417**	N/A	O-MIC-WIND-070920/985
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/986
Improper Input Validation	17-Aug-20	5	A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability'. **CVE ID : CVE-2020-1466**	N/A	O-MIC-WIND-070920/987
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-070920/988

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
			CVE ID : CVE-2020-1467		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**	N/A	O-MIC-WIND-070920/989
Improper Privilege Management	17-Aug-20	9.3	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1472**	N/A	O-MIC-WIND-070920/990
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**	N/A	O-MIC-WIND-070920/991
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the	N/A	O-MIC-WIND-070920/992

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
			Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/993
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	O-MIC-WIND-070920/994
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**	N/A	O-MIC-WIND-070920/995

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
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**	N/A	O-MIC-WIND-070920/996
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1479**	N/A	O-MIC-WIND-070920/997
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1529. **CVE ID : CVE-2020-1480**	N/A	O-MIC-WIND-070920/998
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of	N/A	O-MIC-WIND-070920/999

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
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**	N/A	O-MIC-WIND-070920/1000
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**	N/A	O-MIC-WIND-070920/1001
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1487**	N/A	O-MIC-WIND-070920/1002
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in	N/A	O-MIC-WIND-070920/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1488**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**	N/A	O-MIC-WIND-070920/1004
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1490**	N/A	O-MIC-WIND-070920/1005
Improper Restriction of Operations within the	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in	N/A	O-MIC-WIND-070920/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1492**		
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/1007
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1511**	N/A	O-MIC-WIND-070920/1008
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC	N/A	O-MIC-WIND-070920/1009

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 Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489. **CVE ID : CVE-2020-1513**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1480. **CVE ID : CVE-2020-1529**	N/A	O-MIC-WIND-070920/1010
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**	N/A	O-MIC-WIND-070920/1011
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1531**	N/A	O-MIC-WIND-070920/1012

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 Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1556. **CVE ID : CVE-2020-1533**	N/A	O-MIC-WIND-070920/1013
Improper Privilege Management	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1534**	N/A	O-MIC-WIND-070920/1014
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**	N/A	O-MIC-WIND-070920/1015
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-070920/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows WaasMedic Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows WaasMedic Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1548**	N/A	O-MIC-WIND-070920/1017
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CDP User Components Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1550. **CVE ID : CVE-2020-1549**	N/A	O-MIC-WIND-070920/1018
Improper Restriction of Operations within the Bounds of a	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory.To exploit	N/A	O-MIC-WIND-070920/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CDP User Components Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1549. **CVE ID : CVE-2020-1550**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **CVE ID : CVE-2020-1554**	N/A	O-MIC-WIND-070920/1020
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1533. **CVE ID : CVE-2020-1556**	N/A	O-MIC-WIND-070920/1021
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-070920/1022

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
			2020-1473, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1557**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**	N/A	O-MIC-WIND-070920/1023
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1562. **CVE ID : CVE-2020-1561**	N/A	O-MIC-WIND-070920/1024
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1561. **CVE ID : CVE-2020-1562**	N/A	O-MIC-WIND-070920/1025
Improper Restriction of Operations within the Bounds of a	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database	N/A	O-MIC-WIND-070920/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1558. **CVE ID : CVE-2020-1564**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1565**	N/A	O-MIC-WIND-070920/1027
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1486. **CVE ID : CVE-2020-1566**	N/A	O-MIC-WIND-070920/1028
Improper Input Validation	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**	N/A	O-MIC-WIND-070920/1029

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 Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1568**	N/A	O-MIC-WIND-070920/1030
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**	N/A	O-MIC-WIND-070920/1031
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1577**	N/A	O-MIC-WIND-070920/1032
Information Exposure	17-Aug-20	1.9	An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1578**	N/A	O-MIC-WIND-070920/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**	N/A	O-MIC-WIND-070920/1034
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/1035
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1587**	N/A	O-MIC-WIND-070920/1036
windows_server_2019					
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when the Windows State Repository	N/A	O-MIC-WIND-070920/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service improperly handles objects in memory, aka 'Windows State Repository Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1512**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Telephony Server improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Telephony Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1515**	N/A	O-MIC-WIND-070920/1038
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1484. **CVE ID : CVE-2020-1516**	N/A	O-MIC-WIND-070920/1039
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-070920/1040

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
			would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1518. **CVE ID : CVE-2020-1517**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows File Server Resource Management Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows File Server Resource Management Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1517. **CVE ID : CVE-2020-1518**	N/A	O-MIC-WIND-070920/1041
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1538. **CVE ID : CVE-2020-1519**	N/A	O-MIC-WIND-070920/1042
Improper Restriction of	17-Aug-20	7.2	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-070920/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1520**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1522. **CVE ID : CVE-2020-1521**	N/A	O-MIC-WIND-070920/1044
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Runtime improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-070920/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1521. **CVE ID : CVE-2020-1522**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Speech Shell Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Speech Shell Components Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1524**	N/A	O-MIC-WIND-070920/1046
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1554. **CVE ID : CVE-2020-1525**	N/A	O-MIC-WIND-070920/1047
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Network Connection Broker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Connection Broker Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-070920/1048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1526		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Custom Protocol Engine improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Custom Protocol Engine Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1527**	N/A	O-MIC-WIND-070920/1049
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Radio Manager API improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Radio Manager API Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1528**	N/A	O-MIC-WIND-070920/1050
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Work Folder Service improperly handles file operations, aka 'Windows Work Folder Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1552**	N/A	O-MIC-WIND-070920/1051
Improper Restriction of Operations within the Bounds of a	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-070920/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Runtime Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1553**		
N/A	17-Aug-20	9.3	A remote code execution vulnerability exists when Microsoft .NET Framework processes input, aka '.NET Framework Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1046**	N/A	O-MIC-WIND-070920/1053
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1337**	N/A	O-MIC-WIND-070920/1054
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects, aka 'Windows Media Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1339**	N/A	O-MIC-WIND-070920/1055
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1378. **CVE ID : CVE-2020-1377**	N/A	O-MIC-WIND-070920/1056
Improper Privilege	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-070920/1057

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
Management			Windows Kernel API improperly handles registry objects in memory, aka 'Windows Registry Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1377. **CVE ID : CVE-2020-1378**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1379**	N/A	O-MIC-WIND-070920/1058
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1555, CVE-2020-1570. **CVE ID : CVE-2020-1380**	N/A	O-MIC-WIND-070920/1059
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists in RPC if the server has Routing and Remote Access enabled, aka 'Windows RRAS Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1383**	N/A	O-MIC-WIND-070920/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1486, CVE-2020-1566. **CVE ID : CVE-2020-1417**	N/A	O-MIC-WIND-070920/1061
Improper Verification of Cryptographic Signature	17-Aug-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-1464**	N/A	O-MIC-WIND-070920/1062
Improper Input Validation	17-Aug-20	5	A denial of service vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability'. **CVE ID : CVE-2020-1466**	N/A	O-MIC-WIND-070920/1063
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles hard links, aka 'Windows Hard Link Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1467**	N/A	O-MIC-WIND-070920/1064
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles	N/A	O-MIC-WIND-070920/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1484, CVE-2020-1516. **CVE ID : CVE-2020-1470**		
Improper Privilege Management	17-Aug-20	9.3	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1472**	N/A	O-MIC-WIND-070920/1066
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1557, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1473**	N/A	O-MIC-WIND-070920/1067
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service	N/A	O-MIC-WIND-070920/1068

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 Vulnerability'. This CVE ID is unique from CVE-2020-1485. **CVE ID : CVE-2020-1474**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the srmsvc.dll handles objects in memory, aka 'Windows Server Resource Management Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1475**	N/A	O-MIC-WIND-070920/1069
Improper Privilege Management	17-Aug-20	2.1	An elevation of privilege vulnerability exists when ASP.NET or .NET web applications running on IIS improperly allow access to cached files, aka 'ASP.NET and .NET Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1476**	N/A	O-MIC-WIND-070920/1070
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1477**	N/A	O-MIC-WIND-070920/1071
Improper Restriction of Operations within the Bounds of a	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media	N/A	O-MIC-WIND-070920/1072

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
Memory Buffer			Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1492, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1478**		
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1479**	N/A	O-MIC-WIND-070920/1073
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1529. **CVE ID : CVE-2020-1480**	N/A	O-MIC-WIND-070920/1074
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Work Folders Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Work Folders Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1470, CVE-2020-1516. **CVE ID : CVE-2020-1484**	N/A	O-MIC-WIND-070920/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows Image Acquisition (WIA) Service improperly discloses contents of its memory, aka 'Windows Image Acquisition Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1474. **CVE ID : CVE-2020-1485**	N/A	O-MIC-WIND-070920/1076
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1566. **CVE ID : CVE-2020-1486**	N/A	O-MIC-WIND-070920/1077
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory, aka 'Media Foundation Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1487**	N/A	O-MIC-WIND-070920/1078
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted	N/A	O-MIC-WIND-070920/1079

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
			application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1488**		
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1513. **CVE ID : CVE-2020-1489**	N/A	O-MIC-WIND-070920/1080
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1490**	N/A	O-MIC-WIND-070920/1081
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-070920/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1525, CVE-2020-1554. **CVE ID : CVE-2020-1492**		
Improper Privilege Management	17-Aug-20	6.5	An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1509**	N/A	O-MIC-WIND-070920/1083
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1511**	N/A	O-MIC-WIND-070920/1084
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows CSC Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CSC Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1489. **CVE ID : CVE-2020-1513**	N/A	O-MIC-WIND-070920/1085

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 Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1480. **CVE ID : CVE-2020-1529**	N/A	O-MIC-WIND-070920/1086
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when Windows Remote Access improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1537. **CVE ID : CVE-2020-1530**	N/A	O-MIC-WIND-070920/1087
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Accounts Control improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Accounts Control Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1531**	N/A	O-MIC-WIND-070920/1088
Improper Restriction of Operations within the	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects	N/A	O-MIC-WIND-070920/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1556. **CVE ID : CVE-2020-1533**		
Improper Privilege Management	17-Aug-20	6.8	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1534**	N/A	O-MIC-WIND-070920/1090
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows Remote Access improperly handles file operations, aka 'Windows Remote Access Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1530. **CVE ID : CVE-2020-1537**	N/A	O-MIC-WIND-070920/1091
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-070920/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-1519. **CVE ID : CVE-2020-1538**		
Information Exposure	17-Aug-20	2.1	An information disclosure vulnerability exists when the Windows WaasMedic Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows WaasMedic Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1548**	N/A	O-MIC-WIND-070920/1093
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CDP User Components Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1550. **CVE ID : CVE-2020-1549**	N/A	O-MIC-WIND-070920/1094
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows CDP User Components improperly handle memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows CDP	N/A	O-MIC-WIND-070920/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User Components Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1549. **CVE ID : CVE-2020-1550**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1379, CVE-2020-1477, CVE-2020-1478, CVE-2020-1492, CVE-2020-1525. **CVE ID : CVE-2020-1554**	N/A	O-MIC-WIND-070920/1096
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1570. **CVE ID : CVE-2020-1555**	N/A	O-MIC-WIND-070920/1097
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1533. **CVE ID : CVE-2020-1556**	N/A	O-MIC-WIND-070920/1098

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 Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1558, CVE-2020-1564. **CVE ID : CVE-2020-1557**	N/A	O-MIC-WIND-070920/1099
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1564. **CVE ID : CVE-2020-1558**	N/A	O-MIC-WIND-070920/1100
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1562. **CVE ID : CVE-2020-1561**	N/A	O-MIC-WIND-070920/1101
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-070920/1102

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
			This CVE ID is unique from CVE-2020-1561. **CVE ID : CVE-2020-1562**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1473, CVE-2020-1557, CVE-2020-1558. **CVE ID : CVE-2020-1564**	N/A	O-MIC-WIND-070920/1103
Improper Privilege Management	17-Aug-20	4.6	An elevation of privilege vulnerability exists when the &quot;Public Account Pictures&quot; folder improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1565**	N/A	O-MIC-WIND-070920/1104
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1417, CVE-2020-1486. **CVE ID : CVE-2020-1566**	N/A	O-MIC-WIND-070920/1105
Improper Input	17-Aug-20	7.6	A remote code execution vulnerability exists in the way	N/A	O-MIC-WIND-

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			that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1567**		070920/1106
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1568**	N/A	O-MIC-WIND-070920/1107
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1569**	N/A	O-MIC-WIND-070920/1108
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1380, CVE-2020-1555. **CVE ID : CVE-2020-1570**	N/A	O-MIC-WIND-070920/1109
Information Exposure	17-Aug-20	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite	N/A	O-MIC-WIND-070920/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1577**		
Information Exposure	17-Aug-20	1.9	An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1578**	N/A	O-MIC-WIND-070920/1111
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Function Discovery SSDP Provider improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1579**	N/A	O-MIC-WIND-070920/1112
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists in the way that the dnsrslvr.dll handles objects in memory, aka 'Windows dnsrslvr.dll Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1584**	N/A	O-MIC-WIND-070920/1113
Improper Privilege Management	17-Aug-20	7.2	An elevation of privilege vulnerability exists when the Windows Ancillary Function Driver for WinSock	N/A	O-MIC-WIND-070920/1114

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
			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1587**		
moog					
exvf5c-2_firmware					
Improper Authentication	21-Aug-20	10	The Moog EXO Series EXVF5C-2 and EXVP7C2-3 units support the ONVIF interoperability IP-based physical security protocol, which requires authentication for some of its operations. It was found that the authentication check for those ONVIF operations can be bypassed. An attacker can abuse this issue to execute privileged operations without authentication, for instance, to create a new Administrator user. **CVE ID : CVE-2020-24051**	N/A	O-MOO-EXVF-070920/1115
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	Several XML External Entity (XXE) vulnerabilities in the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units allow remote unauthenticated users to read arbitrary files via a crafted Document Type Definition (DTD) in an XML request. **CVE ID : CVE-2020-24052**	N/A	O-MOO-EXVF-070920/1116

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-20	5	Moog EXO Series EXVF5C-2 and EXVP7C2-3 units have a hardcoded credentials vulnerability. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24053**	N/A	O-MOO-EXVF-070920/1117
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-20	10	The administration console of the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units features a 'statusbroadcast' command that can spawn a given process repeatedly at a certain time interval as 'root'. One of the limitations of this feature is that it only takes a path to a binary without arguments; however, this can be circumvented using special shell variables, such as '${IFS}'. As a result, an attacker can execute arbitrary commands as 'root' on the units. **CVE ID : CVE-2020-24054**	N/A	O-MOO-EXVF-070920/1118
exvp7c2-3_firmware					
Improper Authentication	21-Aug-20	10	The Moog EXO Series EXVF5C-2 and EXVP7C2-3 units support the ONVIF interoperability IP-based physical security protocol, which requires authentication for some of its operations. It was found that the authentication check for those ONVIF operations can be bypassed. An attacker can abuse this issue to execute privileged operations without	N/A	O-MOO-EXVP-070920/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication, for instance, to create a new Administrator user. **CVE ID : CVE-2020-24051**		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	Several XML External Entity (XXE) vulnerabilities in the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units allow remote unauthenticated users to read arbitrary files via a crafted Document Type Definition (DTD) in an XML request. **CVE ID : CVE-2020-24052**	N/A	O-MOO-EXVP-070920/1120
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-20	5	Moog EXO Series EXVF5C-2 and EXVP7C2-3 units have a hardcoded credentials vulnerability. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24053**	N/A	O-MOO-EXVP-070920/1121
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-20	10	The administration console of the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units features a 'statusbroadcast' command that can spawn a given process repeatedly at a certain time interval as 'root'. One of the limitations of this feature is that it only takes a path to a binary without arguments; however, this can be circumvented using special shell variables, such as '${IFS}'. As a result, an attacker can execute arbitrary commands as 'root' on the units.	N/A	O-MOO-EXVP-070920/1122

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-2020-24054		
NCR					
aptra_xfs					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Aug-20	7.2	NCR SelfServ ATMs running APTRA XFS 05.01.00 or earlier do not authenticate or protect the integrity of USB HID communications between the currency dispenser and the host computer, permitting an attacker with physical access to internal ATM components the ability to inject a malicious payload and execute arbitrary code with SYSTEM privileges on the host computer by causing a buffer overflow on the host. **CVE ID : CVE-2020-9063**	N/A	O-NCR-APTR-070920/1123
Improper Authentication	21-Aug-20	2.1	The currency dispenser of NCR SelfSev ATMs running APTRA XFS 05.01.00 or earlier does not adequately authenticate session key generation requests from the host computer, allowing an attacker with physical access to internal ATM components to issue valid commands to dispense currency by generating a new session key that the attacker knows. **CVE ID : CVE-2020-10123**	N/A	O-NCR-APTR-070920/1124
Missing Encryption of Sensitive Data	21-Aug-20	4.4	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not encrypt, authenticate, or verify the integrity of messages between the BNA and the host computer, which	N/A	O-NCR-APTR-070920/1125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker with physical access to the internal components of the ATM to execute arbitrary code, including code that enables the attacker to commit deposit forgery. **CVE ID : CVE-2020-10124**		
Inadequate Encryption Strength	21-Aug-20	4.6	NCR SelfServ ATMs running APTRA XFS 04.02.01 and 05.01.00 implement 512-bit RSA certificates to validate bunch note acceptor (BNA) software updates, which can be broken by an attacker with physical access in a sufficiently short period of time, thereby enabling the attacker to sign arbitrary files and CAB archives used to update BNA software, as well as bypass application whitelisting, resulting in the ability to execute arbitrary code. **CVE ID : CVE-2020-10125**	N/A	O-NCR-APTR-070920/1126
Improper Authentication	21-Aug-20	7.2	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not properly validate softare updates for the bunch note acceptor (BNA), enabling an attacker with physical access to internal ATM components to restart the host computer and execute arbitrary code with SYSTEM privileges because while booting, the update process looks for CAB archives on removable media and executes a specific file	N/A	O-NCR-APTR-070920/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without first validating the signature of the CAB archive. **CVE ID : CVE-2020-10126**		
Netgear					
r6700_firmware					
Use of Externally-Controlled Format String	20-Aug-20	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9755. **CVE ID : CVE-2020-15634**	N/A	O-NET-R670-070920/1128
Stack-based Buffer Overflow	20-Aug-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the acsd service, which listens on TCP port 5916 by default. The issue results from the	N/A	O-NET-R670-070920/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-9853. **CVE ID : CVE-2020-15635**		
Stack-based Buffer Overflow	20-Aug-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR R6400, R6700, R7000, R7850, R7900, R8000, RS400, and XR300 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the check_ra service. A crafted raePolicyVersion in a RAE_Policy.json file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9852. **CVE ID : CVE-2020-15636**	N/A	O-NET-R670-070920/1130
noviflow					
noviware					
Improper Neutralization of Special Elements used in an OS Command	17-Aug-20	8	The novish command-line interface, included in NoviFlow NoviWare before NW500.2.12 and deployed on NoviSwitch devices, is vulnerable to command	N/A	O-NOV-NOVI-070920/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			injection in the "show status destination ipaddr" command. This could be used by a read-only user (monitoring group) or admin to execute commands on the operating system. **CVE ID : CVE-2020-13122**		
openrobotics					
robot_operating_system					
Improper Input Validation	20-Aug-20	6.5	Use of unsafe yaml load. Allows instantiation of arbitrary objects. The flaw itself is caused by an unsafe parsing of YAML values which happens whenever an action message is processed to be sent, and allows for the creation of Python objects. Through this flaw in the ROS core package of actionlib, an attacker with local or remote access can make the ROS Master, execute arbitrary code in Python form. Consider yaml.safe_load() instead. Located first in actionlib/tools/library.py:132. See links for more info on the bug. **CVE ID : CVE-2020-10289**	https://github.com/ros/actionlib/pull/171	O-OPE-ROBO-070920/1132
Opensuse					
leap					
Improper Neutralization of Special Elements used in an SQL	24-Aug-20	6.5	It was found that PostgreSQL versions before 12.4, before 11.9 and before 10.14 did not properly sanitize the search_path during logical replication. An authenticated	N/A	O-OPE-LEAP-070920/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			attacker could use this flaw in an attack similar to CVE-2018-1058, in order to execute arbitrary SQL command in the context of the user used for replication. **CVE ID : CVE-2020-14349**		
Untrusted Search Path	24-Aug-20	4.4	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension. This affects PostgreSQL versions before 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23. **CVE ID : CVE-2020-14350**	N/A	O-OPE-LEAP-070920/1134
NULL Pointer Dereference	19-Aug-20	7.2	A flaw null pointer dereference in the Linux kernel cgroupv2 subsystem in versions before 5.7.10 was found in the way when reboot the system. A local user could use this flaw to crash the system or escalate their privileges on the system. **CVE ID : CVE-2020-14356**	N/A	O-OPE-LEAP-070920/1135
Philips					
suresigns_vs4_firmware					
Improper Input Validation	21-Aug-20	2.1	Philips SureSigns VS4, A.07.107 and prior. The product receives input or data, but it does not validate or incorrectly validates that	N/A	O-PHI-SURE-070920/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the input has the properties required to process the data safely and correctly. **CVE ID : CVE-2020-16237**		
Improper Authentication	21-Aug-20	4	Philips SureSigns VS4, A.07.107 and prior. When an actor claims to have a given identity, the software does not prove or insufficiently proves the claim is correct. **CVE ID : CVE-2020-16239**	N/A	O-PHI-SURE-070920/1137
Incorrect Authorization	21-Aug-20	2.1	Philips SureSigns VS4, A.07.107 and prior. The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor. **CVE ID : CVE-2020-16241**	N/A	O-PHI-SURE-070920/1138
rangee					
rangeeos					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Aug-20	7.2	In the default configuration of Rangee GmbH RangeeOS 8.0.4, all components are executed in the context of the privileged root user. This may allow a local attacker to break out of the restricted environment or inject malicious code into the application and fully compromise the operating system. **CVE ID : CVE-2020-16282**	N/A	O-RAN-RANG-070920/1139
Redhat					
virtualization					
Improper Neutralizatio	18-Aug-20	4.3	A flaw was found in Ovirt Engine's web interface in	https://bugzilla.redhat.	O-RED-VIRT-070920/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			ovirt 4.4 and earlier, where it did not filter user-controllable parameters completely, resulting in a reflected cross-site scripting attack. This flaw allows an attacker to leverage a phishing attack, steal an unsuspecting user's cookies or other confidential information, or impersonate them within the application's context. **CVE ID : CVE-2020-14333**	com/show_bug.cgi?id=CVE-2020-14333	
enterprise_linux					
NULL Pointer Dereference	19-Aug-20	7.2	A flaw null pointer dereference in the Linux kernel cgroupv2 subsystem in versions before 5.7.10 was found in the way when reboot the system. A local user could use this flaw to crash the system or escalate their privileges on the system. **CVE ID : CVE-2020-14356**	N/A	O-RED-ENTE-070920/1141
secomea					
gatemanager_8250_firmware					
Use of Password Hash With Insufficient Computational Effort	25-Aug-20	5	GateManager versions prior to 9.2c, The affected product uses a weak hash type, which may allow an attacker to view user passwords. **CVE ID : CVE-2020-14512**	N/A	O-SEC-GATE-070920/1142
Seowonintech					
slc-130_firmware					
Improper Control of Generation of Code ('Code	20-Aug-20	7.5	SEOWON INTECH SLC-130 And SLR-120S devices allow Remote Code Execution via the ipAddr parameter to the	N/A	O-SEO-SLC--070920/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			system_log.cgi page. **CVE ID : CVE-2020-17456**		
slr-120s_firmware					
Improper Control of Generation of Code ('Code Injection')	20-Aug-20	7.5	SEOWON INTECH SLC-130 And SLR-120S devices allow Remote Code Execution via the ipAddr parameter to the system_log.cgi page. **CVE ID : CVE-2020-17456**	N/A	O-SEO-SLR--070920/1144
sintef					
urx					
Improper Privilege Management	21-Aug-20	7.2	Universal Robots controller execute URCaps (zip files containing Java-powered applications) without any permission restrictions and a wide API that presents many primitives that can compromise the overall robot operations as demonstrated in our video. In our PoC we demonstrate how a malicious actor could 'cook' a custom URCap that when deployed by the user (intendedly or unintendedly) compromises the system **CVE ID : CVE-2020-10290**	https://github.com/aliasrobotics/RVD/issues/1495	O-SIN-URX-070920/1145
verint					
5620ptz_firmware					
Out-of-bounds Write	21-Aug-20	7.5	Verint 5620PTZ Verint_FW_0_42 and Verint 4320 V4320_FW_0_23, and V4320_FW_0_31 units feature an autodiscovery service implemented in the binary executable '/usr/sbin/DM' that listens on port TCP 6666.	N/A	O-VER-5620-070920/1146

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 service is vulnerable to a stack buffer overflow. It is worth noting that this service does not require any authentication. **CVE ID : CVE-2020-24055**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-20	5	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23, V4320_FW_0_31, and Verint S5120FD Verint_FW_0_42units. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24056**	N/A	O-VER-5620-070920/1147
4320_firmware					
Out-of-bounds Write	21-Aug-20	7.5	Verint 5620PTZ Verint_FW_0_42 and Verint 4320 V4320_FW_0_23, and V4320_FW_0_31 units feature an autodiscovery service implemented in the binary executable '/usr/sbin/DM' that listens on port TCP 6666. The service is vulnerable to a stack buffer overflow. It is worth noting that this service does not require any authentication. **CVE ID : CVE-2020-24055**	N/A	O-VER-4320-070920/1148
Improper Limitation of a Pathname to a Restricted Directory ('Path	21-Aug-20	5	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23, V4320_FW_0_31, and Verint S5120FD Verint_FW_0_42units. This	N/A	O-VER-4320-070920/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24056**		
s5120fd_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-20	5	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23, V4320_FW_0_31, and Verint S5120FD Verint_FW_0_42units. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24056**	N/A	O-VER-S512-070920/1150
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-20	9	The management website of the Verint S5120FD Verint_FW_0_42 unit features a CGI endpoint ('ipfilter.cgi') that allows the user to manage network filtering on the unit. This endpoint is vulnerable to a command injection. An authenticated attacker can leverage this issue to execute arbitrary commands as 'root'. **CVE ID : CVE-2020-24057**	N/A	O-VER-S512-070920/1151
Vmware					
esxi					
Improper Authentication	21-Aug-20	5	VMware ESXi and vCenter Server contain a partial denial of service vulnerability in their respective authentication services. VMware has evaluated the severity of this issue to be in	N/A	O-VMW-ESXI-070920/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Moderate severity range with a maximum CVSSv3 base score of 5.3. **CVE ID : CVE-2020-3976**		
Hardware					
Asus					
rt-ac1900p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-20	4.3	An issue was discovered on ASUS RT-AC1900P routers before 3.0.0.4.385_20253. They allow XSS via spoofed Release Notes on the Firmware Upgrade page. **CVE ID : CVE-2020-15499**	N/A	H-ASU-RT-A-070920/1153
Cisco					
sf250-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	H-CIS-SF25-070920/1154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sf250-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF25-070920/1155
sf250-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	H-CIS-SF25-070920/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf250-48hp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF25-070920/1157
sg250-08					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	H-CIS-SG25-070920/1158

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 Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-08hp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	H-CIS-SG25-070920/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-10p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG25-070920/1160
sg250-18					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	H-CIS-SG25-070920/1161

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
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-26					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG25-070920/1162
sg250-26hp					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	H-CIS-SG25-

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
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/1163
sg250-26p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	H-CIS-SG25-070920/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-50					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG25-070920/1165
sg250-50hp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	H-CIS-SG25-070920/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250-50p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG25-070920/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg250x-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG25-070920/1168
sg250x-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	H-CIS-SG25-070920/1169

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
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg250x-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG25-070920/1170
sg250x-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	H-CIS-SG25-070920/1171

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
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf350-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	H-CIS-SF35-070920/1172

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-2020-3363		
sf350-48mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF35-070920/1173
sf350-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	H-CIS-SF35-070920/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-10					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG35-070920/1175
sg350-10mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	H-CIS-SG35-070920/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-10p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	H-CIS-SG35-070920/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-28					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG35-070920/1178
sg350-28mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	H-CIS-SG35-070920/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350-28p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG35-070920/1180
sg355-10p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	H-CIS-SG35-070920/1181

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 Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf550x-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	H-CIS-SF55-070920/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf550x-24mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF55-070920/1183
sf550x-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	H-CIS-SF55-070920/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf550x-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF55-070920/1185
sf550x-48mp					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	H-CIS-SF55-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/1186
sf550x-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	H-CIS-SF55-070920/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf200-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF20-070920/1188
sf200-24fp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	H-CIS-SF20-070920/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf200-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF20-070920/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf200-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF20-070920/1191
sf200-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	H-CIS-SF20-070920/1192

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
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-08					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG20-070920/1193
sg200-08p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	H-CIS-SG20-070920/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-10fp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	H-CIS-SG20-070920/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3363		
sg200-18					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG20-070920/1196
sg200-26					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	H-CIS-SG20-070920/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-26fp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG20-070920/1198
sg200-26p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	H-CIS-SG20-070920/1199

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
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-50					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	H-CIS-SG20-070920/1200

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
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sg200-50fp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG20-070920/1201
sg200-50p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	H-CIS-SG20-070920/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-08					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF30-070920/1203
sf300-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	H-CIS-SF30-070920/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-24mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	H-CIS-SF30-070920/1205

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. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF30-070920/1206
sf300-24pp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	H-CIS-SF30-070920/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf300-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF30-070920/1208
sf300-48p					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	H-CIS-SF30-

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
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/1209
sf300-48pp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	H-CIS-SF30-070920/1210

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
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf302-08					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF30-070920/1211
sf302-08mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	H-CIS-SF30-070920/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf302-08mpp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF30-070920/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf302-08p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF30-070920/1214
sf302-08pp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	H-CIS-SF30-070920/1215

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
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-10					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG30-070920/1216
sg300-10mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	H-CIS-SG30-070920/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-10mpp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	H-CIS-SG30-070920/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3363		
sg300-10p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG30-070920/1219
sg300-10pp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	H-CIS-SG30-070920/1220

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
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-10sfp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG30-070920/1221
sg300-20					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	H-CIS-SG30-070920/1222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-28					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	H-CIS-SG30-070920/1223

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
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-28mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG30-070920/1224
sg300-28p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	H-CIS-SG30-070920/1225

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
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350xg-24t					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG35-070920/1226
sg350xg-2f10					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	H-CIS-SG35-070920/1227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350xg-48t					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	H-CIS-SG35-070920/1228

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. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
asr_5500					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.8	A vulnerability in the IPv6 implementation of Cisco StarOS could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet to an affected device with the goal of reaching the vulnerable section of the input buffer. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3500**	N/A	H-CIS-ASR_-070920/1229
asr_5700					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Aug-20	7.8	A vulnerability in the IPv6 implementation of Cisco StarOS could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of	N/A	H-CIS-ASR_-070920/1230

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
			incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet to an affected device with the goal of reaching the vulnerable section of the input buffer. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3500**		
sg550x-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG55-070920/1231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg550x-24mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG55-070920/1232
sg550x-24mpp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	H-CIS-SG55-070920/1233

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
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg550x-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG55-070920/1234
sg550x-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	H-CIS-SG55-070920/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg550x-48mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	H-CIS-SG55-070920/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3363		
sg550x-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG55-070920/1237
sx550x-12f					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	H-CIS-SX55-070920/1238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sx550x-16ft					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SX55-070920/1239
sx550x-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	H-CIS-SX55-070920/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sx550x-24f					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	H-CIS-SX55-070920/1241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sx550x-24ft					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SX55-070920/1242
sx550x-52					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	H-CIS-SX55-070920/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350x-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG35-070920/1244
sg350x-24mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	H-CIS-SG35-070920/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350x-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	H-CIS-SG35-070920/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350x-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG35-070920/1247
sg350x-48mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation	N/A	H-CIS-SG35-070920/1248

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
			of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg350x-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG35-070920/1249
sg350xg-24f					
Improper	17-Aug-20	5	A vulnerability in the IPv6	N/A	H-CIS-SG35-

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
Input Validation			packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		070920/1250
sg300-28pp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an	N/A	H-CIS-SG30-070920/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-52					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG30-070920/1252
sg300-52mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	N/A	H-CIS-SG30-070920/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg300-52p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG30-070920/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf500-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF50-070920/1255
sf500-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A	N/A	H-CIS-SF50-070920/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sf500-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SF50-070920/1257
sf500-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a	N/A	H-CIS-SF50-070920/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500-28					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected.	N/A	H-CIS-SG50-070920/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3363		
sg500-28mpp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG50-070920/1260
sg500-28p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through	N/A	H-CIS-SG50-070920/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500-52					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG50-070920/1262
sg500-52mp					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	H-CIS-SG50-070920/1263

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
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500-52p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4	N/A	H-CIS-SG50-070920/1264

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
			traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500x-24					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG50-070920/1265
sg500x-24p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this	N/A	H-CIS-SG50-070920/1266

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
			vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500x-48					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**	N/A	H-CIS-SG50-070920/1267
sg500x-48p					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart	N/A	H-CIS-SG50-070920/1268

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 Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
sg500xg-8f8t					
Improper Input Validation	17-Aug-20	5	A vulnerability in the IPv6 packet processing engine of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient validation of incoming IPv6 traffic. An attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. A successful exploit could allow the attacker to cause an unexpected reboot of the switch, leading to a DoS	N/A	H-CIS-SG50-070920/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is specific to IPv6 traffic. IPv4 traffic is not affected. **CVE ID : CVE-2020-3363**		
dieboldnixdorf					
procash_2100xe					
Missing Encryption of Sensitive Data	21-Aug-20	2.1	Diebold Nixdorf ProCash 2100xe USB ATMs running Wincor Probase version 1.1.30 do not encrypt, authenticate, or verify the integrity of messages between the CCDM and the host computer, allowing an attacker with physical access to internal ATM components to commit deposit forgery by intercepting and modifying messages to the host computer, such as the amount and value of currency being deposited. **CVE ID : CVE-2020-9062**	N/A	H-DIE-PROC-070920/1270
Huawei					
e6878-370					
Incorrect Authorizatio n	17-Aug-20	6.8	Huawei 5G Mobile WiFi E6878-370 with versions of 10.0.3.1(H563SP1C00),10.0.3.1(H563SP21C233) have an improper authorization vulnerability. The device does not restrict certain data received from WAN port. Successful exploit could allow an attacker at WAN side to manage certain service of the device. **CVE ID : CVE-2020-9241**	N/A	H-HUA-E687-070920/1271

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
taurus-al00b					
Use After Free	17-Aug-20	4.6	Huawei smartphone Taurus-AL00B with versions earlier than 10.1.0.126(C00E125R5P3) have a user after free vulnerability. A module is lack of lock protection. Attackers can exploit this vulnerability by launching specific request. This could compromise normal service of the affected device. **CVE ID : CVE-2020-9237**	N/A	H-HUA-TAUR-070920/1272
p30_pro					
Integer Overflow or Wraparound	21-Aug-20	2.1	HUAWEI P30 Pro smartphone with Versions earlier than 10.1.0.160(C00E160R2P8) has an integer overflow vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this vulnerability by send malicious message to cause integer overflow. This can compromise normal service. **CVE ID : CVE-2020-9095**	N/A	H-HUA-P30_-070920/1273
Out-of-bounds Read	21-Aug-20	2.1	HUAWEI P30 Pro smartphones with Versions earlier than 10.1.0.160(C00E160R2P8) have an out of bound read vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this	N/A	H-HUA-P30_-070920/1274

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
			vulnerability by send malicious message to cause out-of-bound read. This can compromise normal service. **CVE ID : CVE-2020-9096**		
p30					
Improper Release of Memory Before Removing Last Reference	21-Aug-20	3.3	HUAWEI P30 smartphones with Versions earlier than 10.1.0.123(C431E22R2P5),Versions earlier than 10.1.0.123(C432E22R2P5),Versions earlier than 10.1.0.126(C10E7R5P1),Versions earlier than 10.1.0.126(C185E4R7P1),Versions earlier than 10.1.0.126(C461E7R3P1),Versions earlier than 10.1.0.126(C605E19R1P3),Versions earlier than 10.1.0.126(C636E7R3P4),Versions earlier than 10.1.0.128(C635E3R2P4),Versions earlier than 10.1.0.160(C00E160R2P11),Versions earlier than 10.1.0.160(C01E160R2P11) have a denial of service vulnerability. In specific scenario, due to the improper resource management and memory leak of some feature, the attacker could exploit this vulnerability to cause the device reset. **CVE ID : CVE-2020-9104**	N/A	H-HUA-P30-070920/1275
mate_20					
N/A	17-Aug-20	2.1	HUAWEI Mate 20 smartphones with	N/A	H-HUA-MATE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.0.0.205(C00E205R2P1) have a logic error vulnerability. In a special scenario, the system does not properly process. As a result, attackers can perform a series of operations to successfully establish P2P connections that are rejected by the peer end. As a result, the availability of the device is affected. **CVE ID : CVE-2020-9103**		070920/1276
IBM					
flashsystem_v5000					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-FLAS-070920/1277
flashsystem_v7200					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-FLAS-070920/1278
flashsystem_v9000					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should	https://www.ibm.com/support/pages/node/6260199	H-IBM-FLAS-070920/1279

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
			not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**		
flashsystem_v9100					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-FLAS-070920/1280
flashsystem_v9200					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-FLAS-070920/1281
san_volume_controller					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-SAN_-070920/1282
storwize_v5000					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-	https://www.ibm.com/support/pages/node/6260199	H-IBM-STOR-070920/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Force ID: 186678. **CVE ID : CVE-2020-4686**		
storwize_v5000e					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-STOR-070920/1284
storwize_v5100					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-STOR-070920/1285
storwize_v7000					
Improper Privilege Management	17-Aug-20	5.5	IBM Spectrum Virtualize 8.3.1 could allow a remote user authenticated via LDAP to escalate their privileges and perform actions they should not have access to. IBM X-Force ID: 186678. **CVE ID : CVE-2020-4686**	https://www.ibm.com/support/pages/node/6260199	H-IBM-STOR-070920/1286
moog					
exvf5c-2					
Improper Authentication	21-Aug-20	10	The Moog EXO Series EXVF5C-2 and EXVP7C2-3 units support the ONVIF interoperability IP-based physical security protocol, which requires authentication	N/A	H-MOO-EXVF-070920/1287

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 some of its operations. It was found that the authentication check for those ONVIF operations can be bypassed. An attacker can abuse this issue to execute privileged operations without authentication, for instance, to create a new Administrator user. **CVE ID : CVE-2020-24051**		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	Several XML External Entity (XXE) vulnerabilities in the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units allow remote unauthenticated users to read arbitrary files via a crafted Document Type Definition (DTD) in an XML request. **CVE ID : CVE-2020-24052**	N/A	H-MOO-EXVF-070920/1288
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-20	5	Moog EXO Series EXVF5C-2 and EXVP7C2-3 units have a hardcoded credentials vulnerability. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24053**	N/A	H-MOO-EXVF-070920/1289
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-20	10	The administration console of the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units features a 'statusbroadcast' command that can spawn a given process repeatedly at a certain time interval as 'root'. One of the limitations of this feature is that it only takes a path to a binary without	N/A	H-MOO-EXVF-070920/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arguments; however, this can be circumvented using special shell variables, such as '${IFS}'. As a result, an attacker can execute arbitrary commands as 'root' on the units. **CVE ID : CVE-2020-24054**		
exvp7c2-3					
Improper Authentication	21-Aug-20	10	The Moog EXO Series EXVF5C-2 and EXVP7C2-3 units support the ONVIF interoperability IP-based physical security protocol, which requires authentication for some of its operations. It was found that the authentication check for those ONVIF operations can be bypassed. An attacker can abuse this issue to execute privileged operations without authentication, for instance, to create a new Administrator user. **CVE ID : CVE-2020-24051**	N/A	H-MOO-EXVP-070920/1291
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	21-Aug-20	6.4	Several XML External Entity (XXE) vulnerabilities in the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units allow remote unauthenticated users to read arbitrary files via a crafted Document Type Definition (DTD) in an XML request. **CVE ID : CVE-2020-24052**	N/A	H-MOO-EXVP-070920/1292
Improper Limitation of a Pathname	21-Aug-20	5	Moog EXO Series EXVF5C-2 and EXVP7C2-3 units have a hardcoded credentials	N/A	H-MOO-EXVP-070920/1293

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
to a Restricted Directory ('Path Traversal')			vulnerability. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24053**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-20	10	The administration console of the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units features a 'statusbroadcast' command that can spawn a given process repeatedly at a certain time interval as 'root'. One of the limitations of this feature is that it only takes a path to a binary without arguments; however, this can be circumvented using special shell variables, such as '${IFS}'. As a result, an attacker can execute arbitrary commands as 'root' on the units. **CVE ID : CVE-2020-24054**	N/A	H-MOO-EXVP-070920/1294
NCR					
selfserv_atm					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Aug-20	7.2	NCR SelfServ ATMs running APTRA XFS 05.01.00 or earlier do not authenticate or protect the integrity of USB HID communications between the currency dispenser and the host computer, permitting an attacker with physical access to internal ATM components the ability to inject a malicious payload and execute arbitrary code with SYSTEM privileges on the host computer by causing a buffer	N/A	H-NCR-SELF-070920/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow on the host. **CVE ID : CVE-2020-9063**		
Improper Authenticatio n	21-Aug-20	2.1	The currency dispenser of NCR SelfSev ATMs running APTRA XFS 05.01.00 or earlier does not adequately authenticate session key generation requests from the host computer, allowing an attacker with physical access to internal ATM components to issue valid commands to dispense currency by generating a new session key that the attacker knows. **CVE ID : CVE-2020-10123**	N/A	H-NCR-SELF-070920/1296
Missing Encryption of Sensitive Data	21-Aug-20	4.4	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not encrypt, authenticate, or verify the integrity of messages between the BNA and the host computer, which could allow an attacker with physical access to the internal components of the ATM to execute arbitrary code, including code that enables the attacker to commit deposit forgery. **CVE ID : CVE-2020-10124**	N/A	H-NCR-SELF-070920/1297
Inadequate Encryption Strength	21-Aug-20	4.6	NCR SelfServ ATMs running APTRA XFS 04.02.01 and 05.01.00 implement 512-bit RSA certificates to validate bunch note acceptor (BNA) software updates, which can be broken by an attacker with physical access in a sufficiently short period of	N/A	H-NCR-SELF-070920/1298

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
			time, thereby enabling the attacker to sign arbitrary files and CAB archives used to update BNA software, as well as bypass application whitelisting, resulting in the ability to execute arbitrary code. **CVE ID : CVE-2020-10125**		
Improper Authentication	21-Aug-20	7.2	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not properly validate softare updates for the bunch note acceptor (BNA), enabling an attacker with physical access to internal ATM components to restart the host computer and execute arbitrary code with SYSTEM privileges because while booting, the update process looks for CAB archives on removable media and executes a specific file without first validating the signature of the CAB archive. **CVE ID : CVE-2020-10126**	N/A	H-NCR-SELF-070920/1299
Netgear					
r6700					
Use of Externally-Controlled Format String	20-Aug-20	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results	N/A	H-NET-R670-070920/1300

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
			from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9755. **CVE ID : CVE-2020-15634**		
Stack-based Buffer Overflow	20-Aug-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the acsd service, which listens on TCP port 5916 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-9853. **CVE ID : CVE-2020-15635**	N/A	H-NET-R670-070920/1301
Stack-based Buffer Overflow	20-Aug-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR R6400, R6700, R7000, R7850, R7900, R8000, RS400, and XR300 routers with firmware	N/A	H-NET-R670-070920/1302

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
			1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the check_ra service. A crafted raePolicyVersion in a RAE_Policy.json file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9852. **CVE ID : CVE-2020-15636**		
Philips					
suresigns_vs4					
Improper Input Validation	21-Aug-20	2.1	Philips SureSigns VS4, A.07.107 and prior. The product receives input or data, but it does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly. **CVE ID : CVE-2020-16237**	N/A	H-PHI-SURE-070920/1303
Improper Authentication	21-Aug-20	4	Philips SureSigns VS4, A.07.107 and prior. When an actor claims to have a given identity, the software does not prove or insufficiently proves the claim is correct. **CVE ID : CVE-2020-16239**	N/A	H-PHI-SURE-070920/1304
Incorrect Authorization	21-Aug-20	2.1	Philips SureSigns VS4, A.07.107 and prior. The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.	N/A	H-PHI-SURE-070920/1305

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-2020-16241		
secomea					
gatemanager_8250					
Use of Password Hash With Insufficient Computation al Effort	25-Aug-20	5	GateManager versions prior to 9.2c, The affected product uses a weak hash type, which may allow an attacker to view user passwords. **CVE ID : CVE-2020-14512**	N/A	H-SEC-GATE-070920/1306
Seowonintech					
slc-130					
Improper Control of Generation of Code ('Code Injection')	20-Aug-20	7.5	SEOWON INTECH SLC-130 And SLR-120S devices allow Remote Code Execution via the ipAddr parameter to the system_log.cgi page. **CVE ID : CVE-2020-17456**	N/A	H-SEO-SLC--070920/1307
slr-120s					
Improper Control of Generation of Code ('Code Injection')	20-Aug-20	7.5	SEOWON INTECH SLC-130 And SLR-120S devices allow Remote Code Execution via the ipAddr parameter to the system_log.cgi page. **CVE ID : CVE-2020-17456**	N/A	H-SEO-SLR--070920/1308
ui					
es-12f					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**	N/A	H-UI-ES-1-070920/1309
Improper	17-Aug-20	9	A command injection	N/A	H-UI-ES-1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**		070920/1310
es-16-150w					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**	N/A	H-UI-ES-1-070920/1311
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-1-070920/1312
es-24-250w					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages.	N/A	H-UI-ES-2-070920/1313

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-2020-8232		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-2-070920/1314
es-24-500w					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**	N/A	H-UI-ES-2-070920/1315
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-2-070920/1316
es-24-lite					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information	N/A	H-UI-ES-2-070920/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through SNMP community pages. **CVE ID : CVE-2020-8232**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-2-070920/1318
es-48-500w					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**	N/A	H-UI-ES-4-070920/1319
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-4-070920/1320
es-48-750w					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed	N/A	H-UI-ES-4-070920/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-4-070920/1322
es-48-lite					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**	N/A	H-UI-ES-4-070920/1323
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-4-070920/1324
es-8-150w					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in	N/A	H-UI-ES-8-070920/1325

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
			EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-ES-8-070920/1326
ep-16-xg					
Information Exposure	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**	N/A	H-UI-EP-1-070920/1327
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-EP-1-070920/1328
ep-s16					

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	17-Aug-20	4	An information disclosure vulnerability exists in EdgeMax EdgeSwitch firmware v1.9.0 that allowed read only users could obtain unauthorized information through SNMP community pages. **CVE ID : CVE-2020-8232**	N/A	H-UI-EP-S-070920/1329
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Aug-20	9	A command injection vulnerability exists in EdgeSwitch firmware <v1.9.0 that allowed an authenticated read-only user to execute arbitrary shell commands over the HTTP interface, allowing them to escalate privileges. **CVE ID : CVE-2020-8233**	N/A	H-UI-EP-S-070920/1330
verint					
5620ptz					
Out-of-bounds Write	21-Aug-20	7.5	Verint 5620PTZ Verint_FW_0_42 and Verint 4320 V4320_FW_0_23, and V4320_FW_0_31 units feature an autodiscovery service implemented in the binary executable '/usr/sbin/DM' that listens on port TCP 6666. The service is vulnerable to a stack buffer overflow. It is worth noting that this service does not require any authentication. **CVE ID : CVE-2020-24055**	N/A	H-VER-5620-070920/1331
Improper Limitation of a Pathname to a	21-Aug-20	5	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23,	N/A	H-VER-5620-070920/1332

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
Restricted Directory ('Path Traversal')			V4320_FW_0_31, and Verint S5120FD Verint_FW_0_42units. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24056**		
4320					
Out-of-bounds Write	21-Aug-20	7.5	Verint 5620PTZ Verint_FW_0_42 and Verint 4320 V4320_FW_0_23, and V4320_FW_0_31 units feature an autodiscovery service implemented in the binary executable '/usr/sbin/DM' that listens on port TCP 6666. The service is vulnerable to a stack buffer overflow. It is worth noting that this service does not require any authentication. **CVE ID : CVE-2020-24055**	N/A	H-VER-4320-070920/1333
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-20	5	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23, V4320_FW_0_31, and Verint S5120FD Verint_FW_0_42units. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24056**	N/A	H-VER-4320-070920/1334
s5120fd					
Improper Limitation of a Pathname to a Restricted	21-Aug-20	5	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23, V4320_FW_0_31, and Verint	N/A	H-VER-S512-070920/1335

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
Directory ('Path Traversal')			S5120FD Verint_FW_0_42units. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols. **CVE ID : CVE-2020-24056**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-20	9	The management website of the Verint S5120FD Verint_FW_0_42 unit features a CGI endpoint ('ipfilter.cgi') that allows the user to manage network filtering on the unit. This endpoint is vulnerable to a command injection. An authenticated attacker can leverage this issue to execute arbitrary commands as 'root'. **CVE ID : CVE-2020-24057**	N/A	H-VER-S512-070920/1336