



National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

<https://nciipc.gov.in>

01 - 15 Feb 2021

Vol. 08 No. 03

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Application											
1password											
scim_bridge											
Insufficiently Protected Credentials	08-Feb-21	4	1Password SCIM Bridge before 1.6.2 mishandles validation of authenticated requests for log files, leading to disclosure of a TLS private key. CVE ID : CVE-2021-26905	https://support.1password.com/kb/202102/	A-1PA-SCIM-160221/1						
Adobe											
acrobat											
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21035	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/2						
Integer Overflow or Wraparound	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and	https://helpx.adobe.com/security/products/acrobat/apsb21-	A-ADO-ACRO-160221/3						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an Integer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21036	09.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Path Traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21037	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/4
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/5

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21038		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21039	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/6
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/7

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
			interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21040		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21041	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/8
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally escalate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21042	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/9
Out-of-	11-Feb-21	9.3	Acrobat Reader DC versions	https://helpx	A-ADO-ACRO-

CVSS Scoring Scale	0-1	1-2	2-3	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 Write			versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21044	.adobe.com/security/products/acrobat/apsb21-09.html	160221/10
Improper Access Control	11-Feb-21	9.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper access control vulnerability. An unauthenticated attacker could leverage this vulnerability to elevate privileges in the context of the current user. CVE ID : CVE-2021-21045	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/11
Access of Memory Location After End of Buffer	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an memory corruption vulnerability. An	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/12

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21046		
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21017	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/13
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/14

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21021		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21028	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/15
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21033	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/16
Out-of-	11-Feb-21	4.3	Acrobat Reader DC versions	https://helpx	A-ADO-ACRO-

CVSS Scoring Scale	0-1	1-2	2-3	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 Read			versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally elevate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21034	.adobe.com/security/products/acrobat/apsb21-09.html	160221/17
NULL Pointer Dereference	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a null pointer dereference vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve denial of service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21057	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/18
Improper Input Validation	11-Feb-21	4.3	Adobe Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier)	https://helpx.adobe.com/security/products/acrobat	A-ADO-ACRO-160221/19

CVSS Scoring Scale	0-1	1-2	2-3	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 2017.011.30188 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21060	/apSB21-09.html	
Use After Free	11-Feb-21	4.3	Acrobat Pro DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use-after-free vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21061	https://helpx.adobe.com/security/products/acrobat/apSB21-09.html	A-ADO-ACRO-160221/20
acrobat_dc					
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use	https://helpx.adobe.com/security/products/acrobat/apSB21-09.html	A-ADO-ACRO-160221/21

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21035		
Integer Overflow or Wraparound	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Integer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21036	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/22
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Path Traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/23

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
			the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21037		
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21038	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/24
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/25

CVSS Scoring Scale	0-1	1-2	2-3	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 open a malicious file. CVE ID : CVE-2021-21039		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21040	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/26
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21041	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/27
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier),	https://helpx.adobe.com/s	A-ADO-ACRO-160221/28

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally escalate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21042	ucts/acrobat/apsb21-09.html	
Out-of-bounds Write	11-Feb-21	9.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21044	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/29
Improper Access Control	11-Feb-21	9.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/30

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
			improper access control vulnerability. An unauthenticated attacker could leverage this vulnerability to elevate privileges in the context of the current user. CVE ID : CVE-2021-21045	09.html	
Access of Memory Location After End of Buffer	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21046	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/31
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/32

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21017		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21021	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/33
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21028	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/34
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074	https://helpx.adobe.com/s	A-ADO-ACRO-160221/35

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21033	ecurity/prod ucts/acrobat /apsb21- 09.html	
Out-of- bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally elevate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21034	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO- 160221/36
NULL Pointer Dereference	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a null pointer dereference	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO- 160221/37

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve denial of service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2021-21057</p>		
Improper Input Validation	11-Feb-21	4.3	<p>Adobe Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2021-21060</p>	<p>https://helpx.adobe.com/security/products/acrobat/apsb21-09.html</p>	A-ADO-ACRO-160221/38
Use After Free	11-Feb-21	4.3	<p>Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use-after-free vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this</p>	<p>https://helpx.adobe.com/security/products/acrobat/apsb21-09.html</p>	A-ADO-ACRO-160221/39

CVSS Scoring Scale	0-1	1-2	2-3	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 to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21061		
acrobat_reader					
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21035	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/40
Integer Overflow or Wraparound	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Integer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/41

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21036		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Path Traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21037	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/42
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/43

CVSS Scoring Scale	0-1	1-2	2-3	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 open a malicious file. CVE ID : CVE-2021-21038		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21039	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/44
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21040	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/45
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier),	https://helpx.adobe.com/s	A-ADO-ACRO-160221/46

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
			2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21041	ucts/acrobat/apsb21-09.html	
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally escalate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21042	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/47
Out-of-bounds Write	11-Feb-21	9.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/48

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21044		
Improper Access Control	11-Feb-21	9.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper access control vulnerability. An unauthenticated attacker could leverage this vulnerability to elevate privileges in the context of the current user. CVE ID : CVE-2021-21045	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/49
Access of Memory Location After End of Buffer	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/50

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. CVE ID : CVE-2021-21046		
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21017	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/51
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21021	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/52
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074	https://helpx.adobe.com/s	A-ADO-ACRO-160221/53

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21028	ecurity/prod ucts/acrobat /apsb21- 09.html	
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21033	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/54
Out-of- bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/55

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthenticated attacker could leverage this vulnerability to locally elevate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2021-21034</p>		
NULL Pointer Dereference	11-Feb-21	4.3	<p>Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a null pointer dereference vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve denial of service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p>CVE ID : CVE-2021-21057</p>	<p>https://helpx.adobe.com/security/products/acrobat/apsb21-09.html</p>	A-ADO-ACRO-160221/56
Improper Input Validation	11-Feb-21	4.3	<p>Adobe Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose</p>	<p>https://helpx.adobe.com/security/products/acrobat/apsb21-09.html</p>	A-ADO-ACRO-160221/57

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21060		
Use After Free	11-Feb-21	4.3	Acrobat Pro DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use-after-free vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21061	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/58
acrobat_reader_dc					
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/59

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
			issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21035		
Integer Overflow or Wraparound	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Integer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21036	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/60
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Path Traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21037	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/61

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
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21038	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/62
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21039	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/63
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier)	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/64

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
			and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21040	/apsb21-09.html	
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21041	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/65
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/66

CVSS Scoring Scale	0-1	1-2	2-3	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 to locally escalate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21042		
Out-of-bounds Write	11-Feb-21	9.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21044	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/67
Improper Access Control	11-Feb-21	9.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper access control vulnerability. An unauthenticated attacker could leverage this vulnerability to elevate privileges in the context of	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/68

CVSS Scoring Scale	0-1	1-2	2-3	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 current user. CVE ID : CVE-2021-21045		
Access of Memory Location After End of Buffer	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21046	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/69
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21017	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/70
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074	https://helpx.adobe.com/s	A-ADO-ACRO-160221/71

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21021	ecurity/prod ucts/acrobat /apsb21- 09.html	
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21028	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/72
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/73

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21033		
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally elevate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21034	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/74
NULL Pointer Dereference	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a null pointer dereference vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve denial of service in the	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/75

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21057		
Improper Input Validation	11-Feb-21	4.3	Adobe Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21060	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/76
Use After Free	11-Feb-21	4.3	Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use-after-free vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-160221/77

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. CVE ID : CVE-2021-21061		
adobe_consulting_services_commons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Feb-21	4.3	ACS Commons version 4.9.2 (and earlier) suffers from a Reflected Cross-site Scripting (XSS) vulnerability in version-compare and page-compare due to invalid JCR characters that are not handled correctly. An attacker could potentially exploit this vulnerability to inject malicious JavaScript content into vulnerable form fields and execute it within the context of the victim's browser. Exploitation of this issue requires user interaction in order to be successful. CVE ID : CVE-2021-21043	https://github.com/Adobe-Consulting-Services/acs-aem-commons/security/advisories/GHSA-f92j-qf46-p6vm	A-ADO-ADOB-160221/78
Advantech					
iview					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Feb-21	5	Advantech iView versions prior to v5.7.03.6112 are vulnerable to a SQL injection, which may allow an unauthorized attacker to disclose information. CVE ID : CVE-2021-22654	N/A	A-ADV-IVIE-160221/79
Improper Limitation of a Pathname to a Restricted	11-Feb-21	5	Advantech iView versions prior to v5.7.03.6112 are vulnerable to directory traversal, which may allow an attacker to read sensitive	N/A	A-ADV-IVIE-160221/80

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			files. CVE ID : CVE-2021-22656		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Feb-21	7.5	Advantech iView versions prior to v5.7.03.6112 are vulnerable to a SQL injection, which may allow an attacker to escalate privileges to 'Administrator'. CVE ID : CVE-2021-22658	N/A	A-ADV-IVIE-160221/81
apostrophecms					
sanitize-html					
Not Available	08-Feb-21	5	Apostrophe Technologies sanitize-html before 2.3.1 does not properly handle internationalized domain name (IDN) which could allow an attacker to bypass hostname whitelist validation set by the "allowedIframeHostnames" option. CVE ID : CVE-2021-26539	https://github.com/apostrophecms/sanitize-html/pull/458	A-APO-SANI-160221/82
Not Available	08-Feb-21	5	Apostrophe Technologies sanitize-html before 2.3.2 does not properly validate the hostnames set by the "allowedIframeHostnames" option when the "allowIframeRelativeUrls" is set to true, which allows attackers to bypass hostname whitelist for iframe element, related using an src value that starts with "/\example.com".	https://github.com/apostrophecms/sanitize-html/pull/460	A-APO-SANI-160221/83

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-26540		
Bitcoin					
bitcoin					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	7.5	Bitcoin Core before 0.19.0 might allow remote attackers to execute arbitrary code when another application unsafely passes the -platformpluginpath argument to the bitcoin-qt program, as demonstrated by an x-scheme-handler/bitcoin handler for a .desktop file or a web browser. NOTE: the discoverer states "I believe that this vulnerability cannot actually be exploited." CVE ID : CVE-2021-3401	https://github.com/bitcoin/bitcoin/pull/16578	A-BIT-BITC-160221/84
bitovi					
launchpad					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Feb-21	7.5	All versions of package launchpad are vulnerable to Command Injection via stop. CVE ID : CVE-2021-23330	https://github.com/bitovi/launchpad/issues/123%20issuecomment-732188118 , https://github.com/bitovi/launchpad/pull/124 , https://snyk.io/vuln/SNYK-JS-LAUNCHPAD-1044065	A-BIT-LAUN-160221/85
carrierwave_project					
carrierwave					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	08-Feb-21	4	CarrierWave is an open-source RubyGem which provides a simple and flexible way to upload files from Ruby applications. In CarrierWave before versions 1.3.2 and 2.1.1 the download feature has an SSRF vulnerability, allowing attacks to provide DNS entries or IP addresses that are intended for internal use and gather information about the Intranet infrastructure of the platform. This is fixed in versions 1.3.2 and 2.1.1. CVE ID : CVE-2021-21288	https://github.com/carrierwaveuploader/carrierwave/commit/012702eb3ba1663452aa025831caa304d1a665c0 , https://github.com/carrierwaveuploader/carrierwave/security/advisories/GHSA-fwcm-636p-68r5	A-CAR-CARR-160221/86
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Feb-21	7.5	CarrierWave is an open-source RubyGem which provides a simple and flexible way to upload files from Ruby applications. In CarrierWave before versions 1.3.2 and 2.1.1, there is a code injection vulnerability. The "#manipulate!" method inappropriately evals the content of mutation option(:read/:write), allowing attackers to craft a string that can be executed as a Ruby code. If an application developer supplies untrusted inputs to the option, it will lead to remote code execution(RCE). This is fixed in versions 1.3.2 and 2.1.1. CVE ID : CVE-2021-21305	https://github.com/carrierwaveuploader/carrierwave/commit/387116f5c72efa42bc3938d946b4c8d2f22181b7 , https://github.com/carrierwaveuploader/carrierwave/security/advisories/GHSA-cf3w-g86h-35x4	A-CAR-CARR-160221/87

casap_automated_enrollment_system_project

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
casap_automated_enrollment_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-21	3.5	CASAP Automated Enrollment System 1.0 is affected by cross-site scripting (XSS) in users.php. An attacker can steal a cookie to perform user redirection to a malicious website. CVE ID : CVE-2021-3294	http://casap.com	A-CAS-CASA-160221/88
Cesanta					
mongoose					
Out-of-bounds Write	08-Feb-21	6.4	The mg_http_serve_file function in Cesanta Mongoose HTTP server 7.0 is vulnerable to remote OOB write attack via connection request after exhausting memory pool. CVE ID : CVE-2021-26528	N/A	A-CES-MONG-160221/89
Out-of-bounds Write	08-Feb-21	6.4	The mg_tls_init function in Cesanta Mongoose HTTPS server 7.0 and 6.7-6.18 (compiled with mbedTLS support) is vulnerable to remote OOB write attack via connection request after exhausting memory pool. CVE ID : CVE-2021-26529	N/A	A-CES-MONG-160221/90
Out-of-bounds Write	08-Feb-21	6.4	The mg_tls_init function in Cesanta Mongoose HTTPS server 7.0 (compiled with OpenSSL support) is vulnerable to remote OOB write attack via connection request after exhausting memory pool. CVE ID : CVE-2021-26530	N/A	A-CES-MONG-160221/91
chainsafe					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ethermint					
Authentication Bypass by Capture-replay	08-Feb-21	5	Cosmos Network Ethermint <= v0.4.0 is affected by a transaction replay vulnerability in the EVM module. If the victim sends a very large nonce transaction, the attacker can replay the transaction through the application. CVE ID : CVE-2021-25834	N/A	A-CHA-ETHE-160221/92
Authentication Bypass by Capture-replay	08-Feb-21	5	Cosmos Network Ethermint <= v0.4.0 is affected by a cross-chain transaction replay vulnerability in the EVM module. Since ethermint uses the same chainIDEpoch and signature schemes with ethereum for compatibility, a verified signature in ethereum is still valid in ethermint with the same msg content and chainIDEpoch, which enables "cross-chain transaction replay" attack. CVE ID : CVE-2021-25835	https://github.com/cosmos/ethermint/pull/692	A-CHA-ETHE-160221/93
Not Available	08-Feb-21	5	Cosmos Network Ethermint <= v0.4.0 is affected by cache lifecycle inconsistency in the EVM module. The bytecode set in a FAILED transaction wrongfully remains in memory(stateObject.code) and is further written to persistent store at the Endblock stage, which may be utilized to build honeypot contracts. CVE ID : CVE-2021-25836	N/A	A-CHA-ETHE-160221/94

CVSS Scoring Scale	0-1	1-2	2-3	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 Available	08-Feb-21	5	<p>Cosmos Network Ethermint <= v0.4.0 is affected by cache lifecycle inconsistency in the EVM module. Due to the inconsistency between the Storage caching cycle and the Tx processing cycle, Storage changes caused by a failed transaction are improperly reserved in memory. Although the bad storage cache data will be discarded at EndBlock, it is still valid in the current block, which enables many possible attacks such as an "arbitrary mint token".</p> <p>CVE ID : CVE-2021-25837</p>	N/A	A-CHA-ETHE-160221/95
Cisco					
managed_services_accelerator					
Uncontrolled Resource Consumption	04-Feb-21	6.8	<p>A vulnerability in the REST API of Cisco Managed Services Accelerator (MSX) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to the way that the affected software logs certain API requests. An attacker could exploit this vulnerability by sending a flood of crafted API requests to an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-msx-dos-4j7sytvU</p>	A-CIS-MANA-160221/96

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1266		
unified_computing_system_central_software					
Improper Certificate Validation	04-Feb-21	2.7	<p>A vulnerability in the certificate registration process of Cisco Unified Computing System (UCS) Central Software could allow an authenticated, adjacent attacker to register a rogue Cisco Unified Computing System Manager (UCSM). This vulnerability is due to improper certificate validation. An attacker could exploit this vulnerability by sending a crafted HTTP request to the registration API. A successful exploit could allow the attacker to register a rogue Cisco UCSM and gain access to Cisco UCS Central Software data and Cisco UCSM inventory data.</p> <p>CVE ID : CVE-2021-1354</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-invcert-eOpRvCKH</p>	A-CIS-UNIF-160221/97
webex_meetings_server					
Improper Input Validation	04-Feb-21	3.5	<p>A vulnerability in the user interface of Cisco Webex Meetings and Cisco Webex Meetings Server Software could allow an authenticated, remote attacker to inject a hyperlink into a meeting invitation email. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by entering a URL into a field in the user interface. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-linkinj-WWZpVqu9</p>	A-CIS-WEBE-160221/98

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to generate a Webex Meetings invitation email that contains a link to a destination of their choosing. Because this email is sent from a trusted source, the recipient may be more likely to click the link. CVE ID : CVE-2021-1221		
webex_meetings					
Improper Input Validation	04-Feb-21	3.5	A vulnerability in the user interface of Cisco Webex Meetings and Cisco Webex Meetings Server Software could allow an authenticated, remote attacker to inject a hyperlink into a meeting invitation email. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by entering a URL into a field in the user interface. A successful exploit could allow the attacker to generate a Webex Meetings invitation email that contains a link to a destination of their choosing. Because this email is sent from a trusted source, the recipient may be more likely to click the link. CVE ID : CVE-2021-1221	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-linkinj-WWZpVqu9	A-CIS-WEBE-160221/99
delete_account_project					
delete_account					
Improper Neutralization of Input During Web	01-Feb-21	4.3	deleteaccount.php in the Delete Account plugin 1.4 for MyBB allows XSS via the	N/A	A-DEL-DELE-160221/100

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			deleterason parameter. CVE ID : CVE-2021-3350		
Djangoproject					
django					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Feb-21	5	In Django 2.2 before 2.2.18, 3.0 before 3.0.12, and 3.1 before 3.1.6, the django.utils.archive.extract method (used by "startapp --template" and "startproject --template") allows directory traversal via an archive with absolute paths or relative paths with dot segments. CVE ID : CVE-2021-3281	https://docs.djangoproject.com/en/3.1/releases/security/ , https://www.djangoproject.com/weblog/2021/feb/01/security-releases/	A-DJA-DJAN-160221/101
Docker					
docker					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Feb-21	2.7	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability involving the --users-remap option in which access to remapped root allows privilege escalation to real root. When using "--users-remap", if the root user in the remapped namespace has access to the host filesystem they can modify files under "/var/lib/docker/<remapping>" that cause writing files with extended privileges. Versions 20.10.3 and 19.03.15 contain patches that prevent privilege escalation from remapped user.	https://docs.docker.com/engine/release-notes/#20103 , https://github.com/moby/moby/commit/64bd4485b3a66a597c02c95f5776395e540b2c7c , https://github.com/moby/moby/security/advisories/GHSA-7452-xqpj-	A-DOC-DOCK-160221/102

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-21284	6rpc	
Uncontrolled Resource Consumption	02-Feb-21	4.3	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability in which pulling an intentionally malformed Docker image manifest crashes the dockerd daemon. Versions 20.10.3 and 19.03.15 contain patches that prevent the daemon from crashing. CVE ID : CVE-2021-21285	https://docs.docker.com/engine/release-notes/#20103 , https://github.com/moby/moby/commit/8d3179546e79065adefa67cc697c09d0ab137d30 , https://github.com/moby/moby/security/advisories/GHSA-6fj5-m822-rqx8	A-DOC-DOCK-160221/103
dotty_project					
dotty					
Not Available	02-Feb-21	7.5	Prototype pollution vulnerability in 'dotty' versions 0.0.1 through 0.1.0 allows attackers to cause a denial of service and may lead to remote code execution. CVE ID : CVE-2021-25912	https://github.com/deoxxa/dotty/commit/cd997d37917186c131be71501a698803f2b7ebdb	A-DOT-DOTT-160221/104
dynamoosejs					
dynamoose					
Improperly Controlled Modification of Dynamically-	08-Feb-21	7.5	Dynamoose is an open-source modeling tool for Amazon's DynamoDB. In Dynamoose from version 2.0.0 and before version 2.7.0 there was a	https://github.com/dynamoose/dynamoose/commit/324c62b	A-DYN-DYNA-160221/105

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Determined Object Attributes			<p>prototype pollution vulnerability in the internal utility method "lib/utls/object/set.ts". This method is used throughout the codebase for various operations throughout Dynamoose. We have not seen any evidence of this vulnerability being exploited. There is no evidence this vulnerability impacts versions 1.x.x since the vulnerable method was added as part of the v2 rewrite. This vulnerability also impacts v2.x.x beta/alpha versions. Version 2.7.0 includes a patch for this vulnerability.</p> <p>CVE ID : CVE-2021-21304</p>	<p>4709204955931a187362f8999805b1d8e, https://github.com/dynamoose/dynamoose/security/advisories/GHSA-rrqm-p222-8ph2</p>	
emlog					
emlog					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Feb-21	5	<p>emlog v5.3.1 has full path disclosure vulnerability in t/index.php, which allows an attacker to see the path to the webroot/file.</p> <p>CVE ID : CVE-2021-3293</p>	N/A	A-EML-EMLO-160221/106
ezxml_project					
ezxml					
Out-of-bounds Write	08-Feb-21	5.8	<p>The ezxml_toxml function in ezxml 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.</p>	N/A	A-EZX-EZXM-160221/107

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26220		
Out-of-bounds Write	08-Feb-21	5.8	The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool. CVE ID : CVE-2021-26221	N/A	A-EZX-EZXM-160221/108
Out-of-bounds Write	08-Feb-21	5.8	The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool. CVE ID : CVE-2021-26222	N/A	A-EZX-EZXM-160221/109
fortilogger					
fortilogger					
Unrestricted Upload of File with Dangerous Type	01-Feb-21	7.5	FortiLogger 4.4.2.2 is affected by Arbitrary File Upload by sending a "Content-Type: image/png" header to Config/SaveUploadedHotspot LogoFile and then visiting Assets/temp/hotspot/img/lo gohotspot.asp. CVE ID : CVE-2021-3378	N/A	A-FOR-FORT-160221/110
Fortinet					
fortiweb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-21	4.3	An improper neutralization of input during web page generation in FortiWeb GUI interface 6.3.0 through 6.3.7 and version before 6.2.4 may allow an unauthenticated, remote attacker to perform a reflected cross site scripting attack (XSS) by injecting malicious payload in different vulnerable API end-points.	https://fortiguard.com/advisory/FG-IR-20-122	A-FOR-FORT-160221/111

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-22122							
fusioncharts										
apexcharts										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Feb-21	4.3	The package apexcharts before 3.24.0 are vulnerable to Cross-site Scripting (XSS) via lack of sanitization of graph legend fields. CVE ID : CVE-2021-23327	https://github.com/apexcharts/apexcharts.js/commit/68f3f34d125719b4767614fe0a595cc65bde1d19 , https://github.com/apexcharts/apexcharts.js/pull/2158 , https://snyk.io/vuln/SNYK-JAVA-ORGWEBJAR-SNPM-1070616 , https://snyk.io/vuln/SNYK-JS-APEXCHARTS-1062708	A-FUS-APEX-160221/112					
gitea										
gitea										
Out-of-bounds Write	05-Feb-21	5	Stack buffer overflow vulnerability in gitea 1.9.0 through 1.13.1 allows remote attackers to cause a denial of service (crash) via vectors related to a file path. CVE ID : CVE-2021-3382	N/A	A-GIT-GITE-160221/113					
gitlog_project										
gitlog										
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Feb-21	7.5	The gitlog function in src/index.ts in gitlog before 4.0.4 has a command injection vulnerability. CVE ID : CVE-2021-26541	https://github.com/domharrington/node-gitlog/pull/65	A-GIT-GITL-160221/114
Gnome					
evolution					
Insufficient Verification of Data Authenticity	01-Feb-21	2.1	** DISPUTED ** GNOME Evolution through 3.38.3 produces a "Valid signature" message for an unknown identifier on a previously trusted key because Evolution does not retrieve enough information from the GnuPG API. NOTE: third parties dispute the significance of this issue, and dispute whether Evolution is the best place to change this behavior. CVE ID : CVE-2021-3349	N/A	A-GNO-EVOL-160221/115
godotengine					
godot_engine					
Integer Overflow or Wraparound	08-Feb-21	6.8	An integer overflow issue exists in Godot Engine up to v3.2 that can be triggered when loading specially crafted.TGA image files. The vulnerability exists in ImageLoaderTGA::load_image() function at line: const size_t buffer_size = (tga_header.image_width * tga_header.image_height) * pixel_size; The bug leads to	https://github.com/godotengine/godot/pull/45702 , https://github.com/godotengine/godot/pull/45702/files	A-GOD-GODO-160221/116

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Dynamic stack buffer overflow. Depending on the context of the application, attack vector can be local or remote, and can lead to code execution and/or system crash. CVE ID : CVE-2021-26825		
Out-of-bounds Write	08-Feb-21	6.8	A stack overflow issue exists in Godot Engine up to v3.2 and is caused by improper boundary checks when loading .TGA image files. Depending on the context of the application, attack vector can be local or remote, and can lead to code execution and/or system crash. CVE ID : CVE-2021-26826	https://github.com/godotengine/godot/pull/45701 , https://github.com/godotengine/godot/pull/45701/commits/403e4fd08b0b212e96f53d926e6273e0745eaa5a	A-GOD-GODO-160221/117
Google					
chrome					
Improper Privilege Management	09-Feb-21	6.9	Insufficient policy enforcement in Cryptohome in Google Chrome prior to 88.0.4324.96 allowed a local attacker to perform OS-level privilege escalation via a crafted file. CVE ID : CVE-2021-21117	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/118
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Feb-21	6.8	Insufficient data validation in V8 in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-	A-GOO-CHRO-160221/119

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
			CVE ID : CVE-2021-21118	desktop_19.html	
Use After Free	09-Feb-21	6.8	Use after free in Media in Google Chrome prior to 88.0.4324.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21119	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/120
Use After Free	09-Feb-21	6.8	Use after free in WebSQL in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21120	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/121
Use After Free	09-Feb-21	6.8	Use after free in Omnibox in Google Chrome on Linux prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21121	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/122
Use After Free	09-Feb-21	6.8	Use after free in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21122	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/123
Improper	09-Feb-21	4.3	Insufficient data validation in	https://chro	A-GOO-

CVSS Scoring Scale	0-1	1-2	2-3	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			File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. CVE ID : CVE-2021-21123	mereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	CHRO-160221/124
Use After Free	09-Feb-21	6.8	Potential user after free in Speech Recognizer in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21124	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/125
Improper Authentication	09-Feb-21	5.8	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. CVE ID : CVE-2021-21125	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/126
Improper Authentication	09-Feb-21	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension. CVE ID : CVE-2021-21126	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/127
Improper Authentication	09-Feb-21	6.8	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a	https://chromereleases.googleblog.com/2021/01/	A-GOO-CHRO-160221/128

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to bypass content security policy via a crafted Chrome Extension. CVE ID : CVE-2021-21127	stable-channel-update-for-desktop_19.html	
Out-of-bounds Write	09-Feb-21	6.8	Heap buffer overflow in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21128	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/129
Improper Authentication	09-Feb-21	4.3	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. CVE ID : CVE-2021-21129	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/130
Improper Authentication	09-Feb-21	4.3	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. CVE ID : CVE-2021-21130	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/131
Improper Authentication	09-Feb-21	4.3	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/132

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-21131	tml	
Improper Restriction of Rendered UI Layers or Frames	09-Feb-21	6.8	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension. CVE ID : CVE-2021-21132	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/133
Improper Authentication	09-Feb-21	4.3	Insufficient policy enforcement in Downloads in Google Chrome prior to 88.0.4324.96 allowed an attacker who convinced a user to download files to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2021-21133	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/134
Authentication Bypass by Spoofing	09-Feb-21	4.3	Incorrect security UI in Page Info in Google Chrome on iOS prior to 88.0.4324.96 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-21134	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/135
Origin Validation Error	09-Feb-21	4.3	Inappropriate implementation in Performance API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21135	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/136
Origin	09-Feb-21	4.3	Insufficient policy	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-

CVSS Scoring Scale	0-1	1-2	2-3	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 Error			enforcement in WebView in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21136	mereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	CHRO-160221/137
Exposure of Sensitive Information to an Unauthorized Actor	09-Feb-21	4.3	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page. CVE ID : CVE-2021-21137	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/138
Use After Free	09-Feb-21	6.8	Use after free in DevTools in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform a sandbox escape via a crafted file. CVE ID : CVE-2021-21138	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/139
Improper Restriction of Rendered UI Layers or Frames	09-Feb-21	4.3	Inappropriate implementation in iframe sandbox in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2021-21139	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/140
Improper Restriction of Operations within the	09-Feb-21	4.6	Uninitialized use in USB in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially	https://chromereleases.googleblog.com/2021/01/	A-GOO-CHRO-160221/141

CVSS Scoring Scale	0-1	1-2	2-3	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			perform out of bounds memory access via via a USB device. CVE ID : CVE-2021-21140	stable-channel-update-for-desktop_19.html	
Improper Authentication	09-Feb-21	4.3	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass file extension policy via a crafted HTML page. CVE ID : CVE-2021-21141	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	A-GOO-CHRO-160221/142
Use After Free	09-Feb-21	6.8	Use after free in Payments in Google Chrome on Mac prior to 88.0.4324.146 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21142	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-160221/143
Out-of-bounds Write	09-Feb-21	6.8	Heap buffer overflow in Extensions in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. CVE ID : CVE-2021-21143	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-160221/144
Out-of-bounds Write	09-Feb-21	6.8	Heap buffer overflow in Tab Groups in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-	A-GOO-CHRO-160221/145

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption via a crafted Chrome Extension. CVE ID : CVE-2021-21144	desktop.html, https://crbug.com/1163845	
Use After Free	09-Feb-21	6.8	Use after free in Fonts in Google Chrome prior to 88.0.4324.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21145	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-160221/146
Use After Free	09-Feb-21	6.8	Use after free in Navigation in Google Chrome prior to 88.0.4324.146 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21146	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-160221/147
Not Available	09-Feb-21	4.3	Inappropriate implementation in Skia in Google Chrome prior to 88.0.4324.146 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. CVE ID : CVE-2021-21147	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	A-GOO-CHRO-160221/148
Out-of-bounds Write	09-Feb-21	6.8	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.150 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21148	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html	A-GOO-CHRO-160221/149

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Gradle					
enterprise_test_distribution_agent					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Feb-21	5.5	A directory traversal issue was discovered in Gradle gradle-enterprise-test-distribution-agent before 1.3.2, test-distribution-gradle-plugin before 1.3.2, and gradle-enterprise-maven-extension before 1.8.2. A malicious actor (with certain credentials) can perform a registration step such that crafted TAR archives lead to extraction of files into arbitrary filesystem locations. CVE ID : CVE-2021-26719	https://security.gradle.com/advisory/CVE-2021-26719	A-GRA-ENTE-160221/150
test_distribution					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Feb-21	5.5	A directory traversal issue was discovered in Gradle gradle-enterprise-test-distribution-agent before 1.3.2, test-distribution-gradle-plugin before 1.3.2, and gradle-enterprise-maven-extension before 1.8.2. A malicious actor (with certain credentials) can perform a registration step such that crafted TAR archives lead to extraction of files into arbitrary filesystem locations. CVE ID : CVE-2021-26719	https://security.gradle.com/advisory/CVE-2021-26719	A-GRA-TEST-160221/151
maven					
Improper Limitation of	09-Feb-21	5.5	A directory traversal issue was discovered in Gradle	https://security.gradle.com	A-GRA-MAVE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			gradle-enterprise-test-distribution-agent before 1.3.2, test-distribution-gradle-plugin before 1.3.2, and gradle-enterprise-maven-extension before 1.8.2. A malicious actor (with certain credentials) can perform a registration step such that crafted TAR archives lead to extraction of files into arbitrary filesystem locations. CVE ID : CVE-2021-26719	m/advisory/CVE-2021-26719	160221/152

hashicorp

nomad

Not Available	01-Feb-21	5	HashiCorp Nomad and Nomad Enterprise up to 0.12.9 exec and java task drivers can access processes associated with other tasks on the same node. Fixed in 0.12.10, and 1.0.3. CVE ID : CVE-2021-3283	https://discuss.hashicorp.com/t/hcsec-2021-01-nomad-s-exec-and-java-task-drivers-did-not-isolate-processes/20332	A-HAS-NOMA-160221/153
---------------	-----------	---	---	---	-----------------------

vault

Improper Authentication	01-Feb-21	5	HashiCorp Vault Enterprise 1.6.0 & 1.6.1 allowed the `remove-peer` raft operator command to be executed against DR secondaries without authentication. Fixed in 1.6.2. CVE ID : CVE-2021-3282	https://discuss.hashicorp.com/t/hcsec-2021-04-vault-enterprise-s-dr-secondaries-allowed-raft-peer-removal-	A-HAS-VAUL-160221/154
-------------------------	-----------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				without-authenticatio n/20337	
Not Available	01-Feb-21	5	HashiCorp Vault and Vault Enterprise disclosed the internal IP address of the Vault node when responding to some invalid, unauthenticated HTTP requests. Fixed in 1.6.2 & 1.5.7. CVE ID : CVE-2021-3024	<a href="https://discuss.hashicorp.com/t/hcsec-2021-02-vault-api-endpoint-exposed-internal-ip-address-without-authenticatio
n/20334">https://discuss.hashicorp.com/t/hcsec-2021-02-vault-api-endpoint-exposed-internal-ip-address-without-authenticatio n/20334	A-HAS-VAUL-160221/155

helm

helm

Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Feb-21	4	Helm is open-source software which is essentially "The Kubernetes Package Manager". Helm is a tool for managing Charts. Charts are packages of pre-configured Kubernetes resources. In Helm from version 3.0 and before version 3.5.2, there a few cases where data loaded from potentially untrusted sources was not properly sanitized. When a SemVer in the `version` field of a chart is invalid, in some cases Helm allows the string to be used "as is" without sanitizing. Helm fails to properly sanitized some fields present on Helm repository `index.yaml` files. Helm does not properly sanitized some fields in the `plugin.yaml` file	https://github.com/helm/helm/commit/6ce9ba60b73013857e2e7c73d3f86ed70bc1ac9a , https://github.com/helm/helm/security/advisories/GHSA-c38g-469g-cmgx	A-HEL-HELM-160221/156
--	-----------	---	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>for plugins In some cases, Helm does not properly sanitize the fields in the `Chart.yaml` file. By exploiting these attack vectors, core maintainers were able to send deceptive information to a terminal screen running the `helm` command, as well as obscure or alter information on the screen. In some cases, we could send codes that terminals used to execute higher-order logic, like clearing a terminal screen. Further, during evaluation, the Helm maintainers discovered a few other fields that were not properly sanitized when read out of repository index files. This fix remedies all such cases, and once again enforces SemVer2 policies on version fields. All users of the Helm 3 should upgrade to the fixed version 3.5.2 or later. Those who use Helm as a library should verify that they either sanitize this data on their own, or use the proper Helm API calls to sanitize the data.</p> <p>CVE ID : CVE-2021-21303</p>		

henriquedornas

henriquedornas

Improper Neutralization of Input During Web	10-Feb-21	3.5	A stored XSS issue exists in henriquedornas 5.2.17 via online live chat.	N/A	A-HEN-HENR-160221/157
---	-----------	-----	--	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			CVE ID : CVE-2021-26938		
httplib2_project					
httplib2					
Uncontrolled Resource Consumption	08-Feb-21	5	<p>httplib2 is a comprehensive HTTP client library for Python. In httplib2 before version 0.19.0, a malicious server which responds with long series of "\xa0" characters in the "www-authenticate" header may cause Denial of Service (CPU burn while parsing header) of the httplib2 client accessing said server. This is fixed in version 0.19.0 which contains a new implementation of auth headers parsing using the pyparsing library.</p> <p>CVE ID : CVE-2021-21240</p>	<p>https://github.com/httplib2/httplib2/commit/bd9ee252c8f099608019709e22c0d705e98d26bc, https://github.com/httplib2/httplib2/pull/182, https://github.com/httplib2/httplib2/security/advisories/GHSA-93xj-8mrv-444m</p>	A-HTT-HTTP-160221/158
Huawei					
imaster_mae-m					
Improper Privilege Management	06-Feb-21	4.6	<p>There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specific commands to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. Affected product versions include: ManageOne versions</p>	<p>https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-02-privilege-en</p>	A-HUA-IMAS-160221/159

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>6.5.0,6.5.0.SPC100.B210,6.5.1.1.B010,6.5.1.1.B020,6.5.1.1.B030,6.5.1.1.B040,6.5.1.SPC100.B050,6.5.1.SPC101.B010,6.5.1.SPC101.B040,6.5.1.SPC200,6.5.1.SPC200.B010,6.5.1.SPC200.B030,6.5.1.SPC200.B040,6.5.1.SPC200.B050,6.5.1.SPC200.B060,6.5.1.SPC200.B070,6.5.1RC1.B060,6.5.1RC2.B020,6.5.1RC2.B030,6.5.1RC2.B040,6.5.1RC2.B050,6.5.1RC2.B060,6.5.1RC2.B070,6.5.1RC2.B080,6.5.1RC2.B090,6.5.RC2.B050,8.0.0,8.0.0-LCND81,8.0.0.SPC100,8.0.1,8.0.RC2,8.0.RC3,8.0.RC3.B041,8.0.RC3.SPC100;</p> <p>NFV_FusionSphere versions 6.5.1.SPC23,8.0.0.SPC12; SMC2.0 versions V600R019C00,V600R019C10 ; iMaster MAE-M versions MAE-TOOL(FusionSphereBasicTemplate_Euler_X86)V100R020C10SPC220.</p> <p>CVE ID : CVE-2021-22299</p>		

network_functions_virtualization_fusionsphere

Improper Privilege Management	06-Feb-21	4.6	<p>There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specific commands to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. Affected product versions include: ManageOne</p>	<p>https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-02-privilege-en</p>	A-HUA-NETW-160221/160
-------------------------------	-----------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>versions 6.5.0,6.5.0.SPC100.B210,6.5.1 .1.B010,6.5.1.1.B020,6.5.1.1.B 030,6.5.1.1.B040,6.5.1.SPC10 0.B050,6.5.1.SPC101.B010,6.5 .1.SPC101.B040,6.5.1.SPC200, 6.5.1.SPC200.B010,6.5.1.SPC2 00.B030,6.5.1.SPC200.B040,6. 5.1.SPC200.B050,6.5.1.SPC20 0.B060,6.5.1.SPC200.B070,6.5 .1RC1.B060,6.5.1RC2.B020,6. 5.1RC2.B030,6.5.1RC2.B040,6 .5.1RC2.B050,6.5.1RC2.B060, 6.5.1RC2.B070,6.5.1RC2.B080 ,6.5.1RC2.B090,6.5.RC2.B050, 8.0.0,8.0.0- LCND81,8.0.0.SPC100,8.0.1,8. 0.RC2,8.0.RC3,8.0.RC3.B041,8 .0.RC3.SPC100; NFV_FusionSphere versions 6.5.1.SPC23,8.0.0.SPC12; SMC2.0 versions V600R019C00,V600R019C10 ; iMaster MAE-M versions MAE- TOOL(FusionSphereBasicTe mplate_Euler_X86)V100R020 C10SPC220.</p> <p>CVE ID : CVE-2021-22299</p>		

manageone

Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Feb-21	5	<p>Some Huawei products have an inconsistent interpretation of HTTP requests vulnerability. Attackers can exploit this vulnerability to cause information leak. Affected product versions include: CampusInsight versions V100R019C10; ManageOne versions 6.5.1.1,</p>	<p>https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-01-http-en</p>	A-HUA-MANA-160221/161
---	-----------	---	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.5.1.SPC100, 6.5.1.SPC200, 6.5.1RC1, 6.5.1RC2, 8.0.RC2. Affected product versions include: Taurus-AL00A versions 10.0.0.1(C00E1R1P1). CVE ID : CVE-2021-22293		
Not Available	06-Feb-21	4	There is a logic vulnerability in Huawei Gauss100 OLTP Product. An attacker with certain permissions could perform specific SQL statement to exploit this vulnerability. Due to insufficient security design, successful exploit can cause service abnormal. Affected product versions include: ManageOne versions 6.5.1.1.B020, 6.5.1.1.B030, 6.5.1.1.B040, 6.5.1.SPC100.B050, 6.5.1.SPC101.B010, 6.5.1.SPC101.B040, 6.5.1.SPC200, 6.5.1.SPC200.B010, 6.5.1.SPC200.B030, 6.5.1.SPC200.B040, 6.5.1.SPC200.B050, 6.5.1.SPC200.B060, 6.5.1.SPC200.B070, 6.5.1RC1.B070, 6.5.1RC1.B080, 6.5.1RC2.B040, 6.5.1RC2.B050, 6.5.1RC2.B060, 6.5.1RC2.B070, 6.5.1RC2.B080, 6.5.1RC2.B090. CVE ID : CVE-2021-22298	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210113-01-gauss-en	A-HUA-MANA-160221/162

CVSS Scoring Scale	0-1	1-2	2-3	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	06-Feb-21	4.6	<p>There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specific commands to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. Affected product versions include: ManageOne versions</p> <p>6.5.0,6.5.0.SPC100.B210,6.5.1.1.B010,6.5.1.1.B020,6.5.1.1.B030,6.5.1.1.B040,6.5.1.SPC100.B050,6.5.1.SPC101.B010,6.5.1.SPC101.B040,6.5.1.SPC200,6.5.1.SPC200.B010,6.5.1.SPC200.B030,6.5.1.SPC200.B040,6.5.1.SPC200.B050,6.5.1.SPC200.B060,6.5.1.SPC200.B070,6.5.1RC1.B060,6.5.1RC2.B020,6.5.1RC2.B030,6.5.1RC2.B040,6.5.1RC2.B050,6.5.1RC2.B060,6.5.1RC2.B070,6.5.1RC2.B080,6.5.1RC2.B090,6.5.RC2.B050,8.0.0,8.0.0-LCND81,8.0.0.SPC100,8.0.1,8.0.RC2,8.0.RC3,8.0.RC3.B041,8.0.RC3.SPC100;</p> <p>NFV_FusionSphere versions 6.5.1.SPC23,8.0.0.SPC12;</p> <p>SMC2.0 versions V600R019C00,V600R019C10 ; iMaster MAE-M versions MAE-TOOL(FusionSphereBasicTemplate_Euler_X86)V100R020C10SPC220.</p> <p>CVE ID : CVE-2021-22299</p>	<p>https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-02-privilege-en</p>	A-HUA-MANA-160221/163

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
campusinsight										
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Feb-21	5	Some Huawei products have an inconsistent interpretation of HTTP requests vulnerability. Attackers can exploit this vulnerability to cause information leak. Affected product versions include: CampusInsight versions V100R019C10; ManageOne versions 6.5.1.1, 6.5.1.SPC100, 6.5.1.SPC200, 6.5.1RC1, 6.5.1RC2, 8.0.RC2. Affected product versions include: Taurus-AL00A versions 10.0.0.1(C00E1R1P1). CVE ID : CVE-2021-22293	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-01-http-en	A-HUA-CAMP-160221/164					
IBM										
security_verify_information_queue										
Generation of Error Message Containing Sensitive Information	11-Feb-21	4	IBM Security Verify Information Queue 1.0.6 and 1.0.7 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: 196076. CVE ID : CVE-2021-20402	https://exchange.xforce.ibmcloud.com/vulnerabilities/196076 , https://www.ibm.com/support/pages/node/6414361	A-IBM-SECU-160221/165					
Cross-Site Request Forgery (CSRF)	11-Feb-21	6.8	IBM Security Verify Information Queue 1.0.6 and 1.0.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions	https://exchange.xforce.ibmcloud.com/vulnerabilities/196077 , https://www.ibm.com/su	A-IBM-SECU-160221/166					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			transmitted from a user that the website trusts. CVE ID : CVE-2021-20403	ppport/pages/node/6414365	
Not Available	11-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user on the network to cause a denial of service due to an invalid cookie value that could prevent future logins. IBM X-Force ID: 196078. CVE ID : CVE-2021-20404	https://exchange.xforce.ibmcloud.com/vulnerabilities/196078, https://www.ibm.com/support/pages/node/6414363	A-IBM-SECU-160221/167
Improper Encoding or Escaping of Output	11-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user to perform unauthorized activities due to improper encoding of output. IBM X-Force ID: 196183. CVE ID : CVE-2021-20405	https://exchange.xforce.ibmcloud.com/vulnerabilities/196183, https://www.ibm.com/support/pages/node/6414367	A-IBM-SECU-160221/168
Use of a Broken or Risky Cryptographic Algorithm	12-Feb-21	4	IBM Security Verify Information Queue 1.0.6 and 1.0.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 198184. CVE ID : CVE-2021-20406	https://exchange.xforce.ibmcloud.com/vulnerabilities/196184, https://www.ibm.com/support/pages/node/6414763	A-IBM-SECU-160221/169
Cleartext Storage of Sensitive Information	12-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 discloses sensitive information in source code that could be used in further attacks against the system.	https://exchange.xforce.ibmcloud.com/vulnerabilities/196185, https://www	A-IBM-SECU-160221/170

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 198185. CVE ID : CVE-2021-20407	.ibm.com/support/pages/node/6414765	
Cleartext Storage of Sensitive Information	12-Feb-21	2.1	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could disclose highly sensitive information to a local user due to improper storage of a plaintext cryptographic key. IBM X-Force ID: 198187. CVE ID : CVE-2021-20408	https://exchange.xforce.ibmcloud.com/vulnerabilities/196187, https://www.ibm.com/support/pages/node/6414767	A-IBM-SECU-160221/171
Exposure of Sensitive Information to an Unauthorized Actor	12-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 198188. CVE ID : CVE-2021-20409	https://exchange.xforce.ibmcloud.com/vulnerabilities/196188, https://www.ibm.com/support/pages/node/6414771	A-IBM-SECU-160221/172
Cleartext Storage of Sensitive Information	12-Feb-21	3.5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 sends user credentials in plain clear text which can be read by an authenticated user using man in the middle techniques. IBM X-Force ID: 198190. CVE ID : CVE-2021-20410	https://exchange.xforce.ibmcloud.com/vulnerabilities/196190, https://www.ibm.com/support/pages/node/6414773	A-IBM-SECU-160221/173
Incorrect	12-Feb-21	4.8	IBM Security Verify	https://exch	A-IBM-SECU-

CVSS Scoring Scale	0-1	1-2	2-3	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 Transfer Between Spheres			Information Queue 1.0.6 and 1.0.7 could allow a user to impersonate another user on the system due to incorrectly updating the session identifier. IBM X-Force ID: 198191. CVE ID : CVE-2021-20411	ange.xforce.ibmcloud.com/vulnerabilities/196191, https://www.ibm.com/support/pages/node/6414777	160221/174
Use of Hard-coded Credentials	12-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 198192. CVE ID : CVE-2021-20412	https://exchange.xforce.ibmcloud.com/vulnerabilities/196192, https://www.ibm.com/support/pages/node/6414779	A-IBM-SECU-160221/175
websphere_application_server					
Improper Restriction of XML External Entity Reference	10-Feb-21	6.4	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 194882. CVE ID : CVE-2021-20353	https://exchange.xforce.ibmcloud.com/vulnerabilities/194882, https://www.ibm.com/support/pages/node/6413709	A-IBM-WEBS-160221/176
cloud_pak_for_automation					
Cleartext Storage of Sensitive	08-Feb-21	4	IBM Cloud Pak for Automation 20.0.3, 20.0.2-IF002 stores potentially sensitive information in clear	https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-CLOU-160221/177

CVSS Scoring Scale	0-1	1-2	2-3	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			text in API connection log files. This information could be obtained by a user with permissions to read log files. IBM X-Force ID: 194965. CVE ID : CVE-2021-20358	es/194965, https://www.ibm.com/support/pages/node/6412345	
Insertion of Sensitive Information into Log File	08-Feb-21	4	IBM Cloud Pak for Automation 20.0.3, 20.0.2-IF002 - Business Automation Application Designer Component stores potentially sensitive information in log files that could be obtained by an unauthorized user. IBM X-Force ID: 194966. CVE ID : CVE-2021-20359	https://exchange.xforce.ibmcloud.com/vulnerabilities/194966 , https://www.ibm.com/support/pages/node/6412345	A-IBM-CLOU-160221/178
Imagemagick					
imagemagick					
Divide By Zero	06-Feb-21	6.8	A flaw was found in ImageMagick in MagickCore/gem.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior. This flaw affects ImageMagick versions prior to 7.0.10-56. CVE ID : CVE-2021-20176	https://github.com/ImageMagick/ImageMagick/issues/3077	A-IMA-IMAG-160221/179
jenzabar					
jenzabar					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-21	4.3	Jenzabar 9.2.x through 9.2.2 allows /ics?tool=search&query= XSS. CVE ID : CVE-2021-26723	https://jenzabar.com/blog	A-JEN-JENZ-160221/180
Jetbrains					
hub					
URL Redirection to Untrusted Site ('Open Redirect')	03-Feb-21	5.8	In JetBrains Hub before 2020.1.12629, an open redirect was possible. CVE ID : CVE-2021-25757	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-HUB-160221/181
Incorrect Permission Assignment for Critical Resource	03-Feb-21	4	In JetBrains Hub before 2020.1.12629, an authenticated user can delete 2FA settings of any other user. CVE ID : CVE-2021-25759	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-HUB-160221/182
Exposure of Sensitive Information to an Unauthorized Actor	03-Feb-21	5	In JetBrains Hub before 2020.1.12669, information disclosure via the public API was possible. CVE ID : CVE-2021-25760	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-HUB-160221/183
youtrack					
Cross-Site Request Forgery (CSRF)	03-Feb-21	6.8	In JetBrains YouTrack before 2020.4.4701, CSRF via attachment upload was possible. CVE ID : CVE-2021-25765	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-YOUT-160221/184

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
				2020/	
Not Available	03-Feb-21	5	In JetBrains YouTrack before 2020.4.4701, improper resource access checks were made. CVE ID : CVE-2021-25766	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-YOUT-160221/185
Exposure of Sensitive Information to an Unauthorized Actor	03-Feb-21	5	In JetBrains YouTrack before 2020.6.1767, an issue's existence could be disclosed via YouTrack command execution. CVE ID : CVE-2021-25767	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-YOUT-160221/186
Incorrect Permission Assignment for Critical Resource	03-Feb-21	5	In JetBrains YouTrack before 2020.4.4701, permissions for attachments actions were checked improperly. CVE ID : CVE-2021-25768	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-YOUT-160221/187
Not Available	03-Feb-21	5	In JetBrains YouTrack before 2020.4.6808, the YouTrack administrator wasn't able to access attachments. CVE ID : CVE-2021-25769	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-YOUT-160221/188
Improper Control of Generation of Code ('Code Injection')	03-Feb-21	7.5	In JetBrains YouTrack before 2020.5.3123, server-side template injection (SSTI) was possible, which could lead to code execution. CVE ID : CVE-2021-25770	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-YOUT-160221/189
Exposure of Sensitive Information	03-Feb-21	5	In JetBrains YouTrack before 2020.6.1099, project information could be	https://blog.jetbrains.com/blog/2021/	A-JET-YOUT-160221/190

CVSS Scoring Scale	0-1	1-2	2-3	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 an Unauthorized Actor			potentially disclosed. CVE ID : CVE-2021-25771	02/03/jetbrains-security-bulletin-q4-2020/	
ktor					
Use of a Broken or Risky Cryptographic Algorithm	03-Feb-21	5	In JetBrains Ktor before 1.5.0, a birthday attack on SessionStorage key was possible. CVE ID : CVE-2021-25761	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-KTOR-160221/191
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	03-Feb-21	5	In JetBrains Ktor before 1.4.3, HTTP Request Smuggling was possible. CVE ID : CVE-2021-25762	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-KTOR-160221/192
Use of a Broken or Risky Cryptographic Algorithm	03-Feb-21	5	In JetBrains Ktor before 1.4.2, weak cipher suites were enabled by default. CVE ID : CVE-2021-25763	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-KTOR-160221/193
intellij_idea					
Not Available	03-Feb-21	5	In JetBrains IntelliJ IDEA before 2020.2, HTTP links were used for several remote repositories instead of HTTPS. CVE ID : CVE-2021-25756	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-INTE-160221/194
Deserialization of Untrusted Data	03-Feb-21	7.5	In JetBrains IntelliJ IDEA before 2020.3, potentially insecure deserialization of the workspace model could	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-INTE-160221/195

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to code execution. CVE ID : CVE-2021-25758	bulletin-q4-2020/	
teamcity					
Not Available	03-Feb-21	5	In JetBrains TeamCity before 2020.2.2, TeamCity server DoS was possible via server integration. CVE ID : CVE-2021-25772	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-TEAM-160221/196
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-21	4.3	JetBrains TeamCity before 2020.2 was vulnerable to reflected XSS on several pages. CVE ID : CVE-2021-25773	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-TEAM-160221/197
Incorrect Authorization	03-Feb-21	4	In JetBrains TeamCity before 2020.2.1, a user could get access to the GitHub access token of another user. CVE ID : CVE-2021-25774	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-TEAM-160221/198
Incorrect Permission Assignment for Critical Resource	03-Feb-21	5.5	In JetBrains TeamCity before 2020.2.1, the server admin could create and see access tokens for any other users. CVE ID : CVE-2021-25775	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-TEAM-160221/199
Insecure Storage of Sensitive Information	03-Feb-21	5	In JetBrains TeamCity before 2020.2, an ECR token could be exposed in a build's parameters. CVE ID : CVE-2021-25776	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-TEAM-160221/200

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2020/	
Incorrect Authorization	03-Feb-21	5	In JetBrains TeamCity before 2020.2.1, permissions during token removal were checked improperly. CVE ID : CVE-2021-25777	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-TEAM-160221/201
Incorrect Permission Assignment for Critical Resource	03-Feb-21	5	In JetBrains TeamCity before 2020.2.1, permissions during user deletion were checked improperly. CVE ID : CVE-2021-25778	https://blog.jetbrains.com/blog/2021/02/03/jetbrains-security-bulletin-q4-2020/	A-JET-TEAM-160221/202
Linkedin					
oncall					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Feb-21	4.3	LinkedIn Oncall through 1.4.0 allows reflected XSS via /query because of mishandling of the "No results found for" message in the search bar. CVE ID : CVE-2021-26722	N/A	A-LIN-ONCA-160221/203
marked_project					
marked					
Uncontrolled Resource Consumption	08-Feb-21	5	Marked is an open-source markdown parser and compiler (npm package "marked"). In marked from version 1.1.1 and before version 2.0.0, there is a Regular expression Denial of Service vulnerability. This vulnerability can affect anyone who runs user generated code through	https://github.com/markedjs/marked/commit/7293251c438e3ee968970f7609f1a27f9007bccd , https://github.com/markedjs/marked/	A-MAR-MARK-160221/204

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			marked. This vulnerability is fixed in version 2.0.0. CVE ID : CVE-2021-21306	pull/1864, https://github.com/markedjs/marked/security/advisories/GHSA-4r62-v4vq-hr96	

Mcafee

endpoint_security

Improper Privilege Management	10-Feb-21	2.1	Improper Access Control in attribute in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows authenticated local administrator user to perform an uninstallation of the anti-malware engine via the running of a specific command with the correct parameters. CVE ID : CVE-2021-23880	https://kc.mcafee.com/corporate/index?page=content&id=SB10345	A-MCA-ENDP-160221/205
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Feb-21	3.5	A stored cross site scripting vulnerability in ePO extension of McAfee Endpoint Security (ENS) prior to 10.7.0 February 2021 Update allows an ENS ePO administrator to add a script to a policy event which will trigger the script to be run through a browser block page when a local non-administrator user triggers the policy. CVE ID : CVE-2021-23881	https://kc.mcafee.com/corporate/index?page=content&id=SB10345	A-MCA-ENDP-160221/206
Improper Privilege Management	10-Feb-21	1.9	Improper Access Control vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0	https://kc.mcafee.com/corporate/index?page=cont	A-MCA-ENDP-160221/207

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			February 2021 Update allows local administrators to prevent the installation of some ENS files by placing carefully crafted files where ENS will be installed. This is only applicable to clean installations of ENS as the Access Control rules will prevent modification prior to up an upgrade. CVE ID : CVE-2021-23882	ent&id=SB10345	
NULL Pointer Dereference	10-Feb-21	4.9	A Null Pointer Dereference vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update allows a local administrator to cause Windows to crash via a specific system call which is not handled correctly. This varies by machine and had partial protection prior to this update. CVE ID : CVE-2021-23883	https://kc.mcafee.com/corporate/index?page=content&id=SB10345	A-MCA-ENDP-160221/208
total_protection					
Improper Privilege Management	10-Feb-21	4.6	Arbitrary Process Execution vulnerability in McAfee Total Protection (MTP) prior to 16.0.30 allows a local user to gain elevated privileges and execute arbitrary code bypassing MTP self-defense. CVE ID : CVE-2021-23874	http://service.mcafee.com/FAQDocument.aspx?&id=TS103114	A-MCA-TOTA-160221/209
mechanize_project					
mechanize					
Improper Neutralizatio	02-Feb-21	9.3	Mechanize is an open-source ruby library that makes	https://github.com/sparkl	A-MEC-MECH-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			<p>automated web interaction easy. In Mechanize from version 2.0.0 and before version 2.7.7 there is a command injection vulnerability. Affected versions of mechanize allow for OS commands to be injected using several classes' methods which implicitly use Ruby's Kernel.open method. Exploitation is possible only if untrusted input is used as a local filename and passed to any of these calls:</p> <p>Mechanize::CookieJar#load, Mechanize::CookieJar#save_as, Mechanize#download, Mechanize::Download#save, Mechanize::File#save, and Mechanize::FileResponse#read_body. This is fixed in version 2.7.7.</p> <p>CVE ID : CVE-2021-21289</p>	<p>emotion/mechanize/commit/66a6a1bfa653a5f13274a396a5e5441238656aa0,</p> <p>https://github.com/sparklemotion/mechanize/security/advisories/GHSA-qrqm-fpv6-6r8g</p>	160221/210

Microfocus

application_performance_management

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Feb-21	3.5	<p>Persistent Cross-Site scripting vulnerability in Micro Focus Application Performance Management product, affecting versions 9.40, 9.50 and 9.51. The vulnerability could allow persistent XSS attack.</p> <p>CVE ID : CVE-2021-22499</p>	<p>https://software.support.com/doc/KM03775253</p>	A-MIC-APPL-160221/211
Cross-Site Request Forgery (CSRF)	06-Feb-21	4.3	<p>Cross Site Request Forgery vulnerability in Micro Focus Application Performance Management product,</p>	<p>https://software.support.com/doc/KM</p>	A-MIC-APPL-160221/212

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affecting versions 9.40, 9.50 and 9.51. The vulnerability could be exploited by attacker to trick the users into executing actions of the attacker's choosing. CVE ID : CVE-2021-22500	03775253	
operation_bridge_reporter					
Improper Control of Generation of Code ('Code Injection')	08-Feb-21	10	Remote Code execution vulnerability in Micro Focus Operation Bridge Reporter (OBR) product, affecting version 10.40. The vulnerability could be exploited to allow Remote Code Execution on the OBR server. CVE ID : CVE-2021-22502	https://software.support.com/doc/KM03775947	A-MIC-OPER-160221/213
millewin					
millewin					
Incorrect Default Permissions	09-Feb-21	6.5	Millennium Millewin (also known as "Cartella clinica") 13.39.028, 13.39.28.3342, and 13.39.146.1 has insecure folder permissions allowing a malicious user for a local privilege escalation. CVE ID : CVE-2021-3394	N/A	A-MIL-MILL-160221/214
minio					
minio					
Server-Side Request Forgery (SSRF)	01-Feb-21	4	MinIO is a High Performance Object Storage released under Apache License v2.0. In MinIO before version RELEASE.2021-01-30T00-20-58Z there is a server-side request forgery vulnerability.	https://github.com/minio/minio/commit/eb6871ecd960d570f70698877209e6db181bf27	A-MIN-MINI-160221/215

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>The target application may have functionality for importing data from a URL, publishing data to a URL, or otherwise reading data from a URL that can be tampered with. The attacker modifies the calls to this functionality by supplying a completely different URL or by manipulating how URLs are built (path traversal etc.). In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources. The attacker can supply or modify a URL which the code running on the server will read or submit data, and by carefully selecting the URLs, the attacker may be able to read server configuration such as AWS metadata, connect to internal services like HTTP enabled databases, or perform post requests towards internal services which are not intended to be exposed. This is fixed in version RELEASE.2021-01-30T00-20-58Z, all users are advised to upgrade. As a workaround you can disable the browser front-end with "MINIO_BROWSER=off" environment variable.</p> <p>CVE ID : CVE-2021-21287</p>	<p>6, https://github.com/minio/minio/pull/11337, https://github.com/minio/minio/security/advisories/GHSA-m4qq-5f7c-693q</p>	

ms3d_project

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ms3d					
Use of Uninitialized Resource	09-Feb-21	5	An issue was discovered in the ms3d crate before 0.1.3 for Rust. It might allow attackers to obtain sensitive information from uninitialized memory locations via IoReader::read. CVE ID : CVE-2021-26952	https://rustsec.org/advisories/RUSTSEC-2021-0016.html	A-MS3-MS3D-160221/216
Nagios					
favorites					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-21	4.3	The Favorites component before 1.0.2 for Nagios XI 5.8.0 is vulnerable to XSS. CVE ID : CVE-2021-26023	https://www.nagios.com/products/security/	A-NAG-FAVO-160221/217
Not Available	03-Feb-21	5	The Favorites component before 1.0.2 for Nagios XI 5.8.0 is vulnerable to Insecure Direct Object Reference: it is possible to create favorites for any other user account. CVE ID : CVE-2021-26024	https://www.nagios.com/products/security/	A-NAG-FAVO-160221/218
nagios_xi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Feb-21	4.3	The Favorites component before 1.0.2 for Nagios XI 5.8.0 is vulnerable to XSS. CVE ID : CVE-2021-26023	https://www.nagios.com/products/security/	A-NAG-NAGI-160221/219
Not Available	03-Feb-21	5	The Favorites component before 1.0.2 for Nagios XI	https://www.nagios.com/	A-NAG-NAGI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.8.0 is vulnerable to Insecure Direct Object Reference: it is possible to create favorites for any other user account. CVE ID : CVE-2021-26024	products/security/	160221/220
name_directory_project					
name_directory					
Cross-Site Request Forgery (CSRF)	05-Feb-21	6.8	Cross-site request forgery (CSRF) vulnerability in Name Directory 1.17.4 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. CVE ID : CVE-2021-20652	N/A	A-NAM-NAME-160221/221
NCR					
command_center_agent					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Feb-21	10	CMCAgent in NCR Command Center Agent 16.3 on Aloha POS/BOH servers permits the submission of a runCommand parameter (within an XML document sent to port 8089) that enables the remote, unauthenticated execution of an arbitrary command as SYSTEM, as exploited in the wild in 2020 and/or 2021. NOTE: the vendor's position is that exploitation occurs only on devices with a certain "misconfiguration." CVE ID : CVE-2021-3122	N/A	A-NCR-COMM-160221/222
nedi					
nedi					
Improper	12-Feb-21	4	NeDi 1.9C allows an	N/A	A-NED-NEDI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			authenticated user to perform a SQL Injection in the Monitoring History function on the endpoint /Monitoring-History.php via the det HTTP GET parameter. This allows an attacker to access all the data in the database and obtain access to the NeDi application. CVE ID : CVE-2021-26751		160221/223
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-21	6.5	NeDi 1.9C allows an authenticated user to execute operating system commands in the Nodes Traffic function on the endpoint /Nodes-Traffic.php via the md or ag HTTP GET parameter. This allows an attacker to obtain access to the operating system where NeDi is installed and to all application data. CVE ID : CVE-2021-26752	N/A	A-NED-NEDI-160221/224
Improper Control of Generation of Code ('Code Injection')	12-Feb-21	6.5	NeDi 1.9C allows an authenticated user to inject PHP code in the System Files function on the endpoint /System-Files.php via the txt HTTP POST parameter. This allows an attacker to obtain access to the operating system where NeDi is installed and to all application data. CVE ID : CVE-2021-26753	N/A	A-NED-NEDI-160221/225
netmotionsoftware					
netmotion_mobility					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	08-Feb-21	10	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in SupportRpcServlet. CVE ID : CVE-2021-26912	https://www.netmotionsoftware.com/security-advisories/security-vulnerability-in-mobility-web-server-november-19-2020	A-NET-NETM-160221/226
Deserialization of Untrusted Data	08-Feb-21	10	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in RpcServlet. CVE ID : CVE-2021-26913	https://www.netmotionsoftware.com/security-advisories/security-vulnerability-in-mobility-web-server-november-19-2020	A-NET-NETM-160221/227
Deserialization of Untrusted Data	08-Feb-21	10	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in MvcUtil valueStringToObject. CVE ID : CVE-2021-26914	https://www.netmotionsoftware.com/security-advisories/security-vulnerability-in-mobility-web-server-november-19-2020	A-NET-NETM-160221/228
Deserialization of Untrusted Data	08-Feb-21	10	NetMotion Mobility before 11.73 and 12.x before 12.02 allows unauthenticated remote attackers to execute arbitrary code as SYSTEM because of Java deserialization in webrepdb	https://www.netmotionsoftware.com/security-advisories/	A-NET-NETM-160221/229

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			StatusServlet. CVE ID : CVE-2021-26915	in-mobility- web-server- november- 19-2020	
nopcommerce					
nopcommerce					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Feb-21	4.3	In nopCommerce 4.30, a Reflected XSS issue in the Discount Coupon component allows remote attackers to inject arbitrary web script or HTML through the Filters/CheckDiscountCouponAttribute.cs discountcode parameter. CVE ID : CVE-2021-26916	N/A	A-NOP-NOPC-160221/230
Nvidia					
geforce_experience					
Not Available	05-Feb-21	3.6	NVIDIA GeForce Experience, all versions prior to 3.21, contains a vulnerability in GameStream (rxdiag.dll) where an arbitrary file deletion due to improper handling of log files may lead to denial of service. CVE ID : CVE-2021-1072	https://nvidia.custhelp.com/app/answers/detail/a_id/5155	A-NVI-GEFO-160221/231
oauth2_proxy_project					
oauth2_proxy					
URL Redirection to Untrusted Site ('Open Redirect')	02-Feb-21	5.8	OAuth2 Proxy is an open-source reverse proxy and static file server that provides authentication using Providers (Google, GitHub, and others) to validate accounts by email, domain or group. In OAuth2 Proxy	https://github.com/oauth2-proxy/oauth2-proxy/commit/780ae4f3c99b579cb2ea	A-OAU-OAUT-160221/232

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>before version 7.0.0, for users that use the whitelist domain feature, a domain that ended in a similar way to the intended domain could have been allowed as a redirect. For example, if a whitelist domain was configured for ".example.com", the intention is that subdomains of example.com are allowed. Instead, "example.com" and "badexample.com" could also match. This is fixed in version 7.0.0 onwards. As a workaround, one can disable the whitelist domain feature and run separate OAuth2 Proxy instances for each subdomain.</p> <p>CVE ID : CVE-2021-21291</p>	<p>9845121caeb6192f725, https://github.com/oauth2-proxy/oauth2-proxy/security/advisories/GHSA-4mf2-f3wh-gvf2</p>	
Octobercms					
october					
Insufficient Session Expiration	05-Feb-21	6.8	<p>An issue was discovered in October through build 471. It reactivates an old session ID (which had been invalid after a logout) once a new login occurs. NOTE: this violates the intended Auth/Manager.php authentication behavior but, admittedly, is only relevant if an old session ID is known to an attacker.</p> <p>CVE ID : CVE-2021-3311</p>	<p>https://github.com/octobercms/library/commit/642f597489e6f644d4bd9a0c267e864cabead024, https://octobercms.com/forum/chan/announcements</p>	A-OCT-OCTO-160221/233
openhav					
openhav					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	01-Feb-21	4	<p>openHAB is a vendor and technology agnostic open source automation software for your home. In openHAB before versions 2.5.12 and 3.0.1 the XML external entity (XXE) attack allows attackers in the same network as the openHAB instance to retrieve internal information like the content of files from the file system. Responses to SSDP requests can be especially malicious. All add-ons that use SAX or JAXB parsing of externally received XML are potentially subject to this kind of attack. In openHAB, the following add-ons are potentially impacted: AvmFritz, BoseSoundtouch, DenonMarantz, DLinkSmarthome, Enigma2, FmiWeather, FSInternetRadio, Gce, Homematic, HPPrinter, IHC, Insteon, Onkyo, Roku, SamsungTV, Sonos, Roku, Tellstick, TR064, UPnPControl, Vitotronic, Wemo, YamahaReceiver and XPath Transformation. The vulnerabilities have been fixed in versions 2.5.12 and 3.0.1 by a more strict configuration of the used XML parser.</p> <p>CVE ID : CVE-2021-21266</p>	<p>https://github.com/openhab/openhab-addons/commit/81935b0ab126e6d9aebd2f6c3fc67d82bb7e8b86, https://github.com/openhab/openhab-addons/security/advisories/GHSA-r2hc-pmr7-4c9r</p>	A-OPE-OPEN-160221/234
openwrt					
openwrt					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Feb-21	3.3	In OpenWrt 19.07.x before 19.07.7, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set. This affects the netifd and odhcp6c packages. CVE ID : CVE-2021-22161	https://openwrt.org/advistory/2021-02-02-1	A-OPE-OPEN-160221/235
Opmantek					
open-audit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Feb-21	4.3	Opmantek Open-Audit 4.0.1 is affected by cross-site scripting (XSS). When outputting SQL statements for debugging, a maliciously crafted query can trigger an XSS attack. This attack only succeeds if the user is already logged in to Open-Audit before they click the malicious link. CVE ID : CVE-2021-3333	https://community.opmantek.com/display/OA/Errata+-+4.0.1+XSS+input+SQL+debugging+output	A-OPM-OPEN-160221/236
Otrs					
survey					
Improper Neutralization of Input	08-Feb-21	3.5	Survey administrator can craft a survey in such way that malicious code can be	https://otrs.com/release-notes/otrs-	A-OTR-SURV-160221/237

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			executed in the agent interface (i.e. another agent who wants to make changes in the survey). This issue affects: OTRS AG Survey 6.0.x version 6.0.20 and prior versions; 7.0.x version 7.0.19 and prior versions. CVE ID : CVE-2021-21434	security-advisory-2021-01/	
cis_in_customer_frontend					
Incorrect Default Permissions	08-Feb-21	4	Agents are able to see and link Config Items without permissions, which are defined in General Catalog. This issue affects: OTRS AG OTRSCIsInCustomerFrontend 7.0.x version 7.0.14 and prior versions. CVE ID : CVE-2021-21436	https://otrs.com/release-notes/otrs-security-advisory-2021-04/	A-OTR-CIS-160221/238
otrs					
Exposure of Sensitive Information to an Unauthorized Actor	08-Feb-21	4.3	Article Bcc fields and agent personal information are shown when customer prints the ticket (PDF) via external interface. This issue affects: OTRS AG OTRS 7.0.x version 7.0.23 and prior versions; 8.0.x version 8.0.10 and prior versions. CVE ID : CVE-2021-21435	https://otrs.com/release-notes/otrs-security-advisory-2021-02/	A-OTR-OTRS-160221/239
Panasonic					
video_insight_vms					
Improper Control of Generation of Code ('Code Injection')	05-Feb-21	10	Video Insight VMS versions prior to 7.8 allows a remote attacker to execute arbitrary code with the system user privilege by sending a	http://downloadvi.com/downloads/IPServer/v7.8/780182/v78	A-PAN-VIDE-160221/240

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>specialy crafted request.</p> <p>CVE ID : CVE-2021-20623</p>	0182RN.pdf	
peerigon					
angular-expressions					
<p>Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')</p>	01-Feb-21	6.5	<p>angular-expressions is "angular's nicest part extracted as a standalone module for the browser and node". In angular-expressions before version 1.1.2 there is a vulnerability which allows Remote Code Execution if you call "expressions.compile(userControlledInput)" where "userControlledInput" is text that comes from user input. The security of the package could be bypassed by using a more complex payload, using a ".constructor.constructor" technique. In terms of impact: If running angular-expressions in the browser, an attacker could run any browser script when the application code calls expressions.compile(userControlledInput). If running angular-expressions on the server, an attacker could run any Javascript expression, thus gaining Remote Code Execution. This is fixed in version 1.1.2 of angular-expressions A temporary workaround might be either to disable user-controlled input that will be fed into angular-expressions in your</p>	<p>http://blog.angularjs.org/2016/09/angular-16-expression-sandbox-removal.html</p> <p>, https://github.com/peerigon/angular-expressions/commit/07edb62902b1f6127b3dcc013da61c6316dd0bf1</p>	A-PEE-ANGU-160221/241

CVSS Scoring Scale	0-1	1-2	2-3	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 or allow only following characters in the userControlledInput. CVE ID : CVE-2021-21277		
podman_project					
podman					
Origin Validation Error	02-Feb-21	5	Rootless containers run with Podman, receive all traffic with a source IP address of 127.0.0.1 (including from remote hosts). This impacts containerized applications that trust localhost (127.0.0.1) connections by default and do not require authentication. This issue affects Podman 1.8.0 onwards. CVE ID : CVE-2021-20199	https://github.com/containers/podman/pull/9052 , https://github.com/rootless-containers/rootlesskit/pull/206	A-POD-PODM-160221/242
polrproject					
polr					
Incorrect Authorization	01-Feb-21	6.4	Polr is an open source URL shortener. in Polr before version 2.3.0, a vulnerability in the setup process allows attackers to gain admin access to site instances, even if they do not possess an existing account. This vulnerability exists regardless of users' settings. If an attacker crafts a request with specific cookie headers to the /setup/finish endpoint, they may be able to obtain admin privileges on the instance. This is caused by a loose comparison (==) in	https://github.com/cydrbolt/polr/commit/b1981709908caf6069b4a29dad3b6739c322c675 , https://github.com/cydrbolt/polr/security/advisories/GHSA-vg6w-8w9v-xxqc	A-POL-POLR-160221/243

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SetupController that is susceptible to attack. The project has been patched to ensure that a strict comparison (===) is used to verify the setup key, and that /setup/finish verifies that no users table exists before performing any migrations or provisioning any new accounts. This is fixed in version 2.3.0. Users can patch this vulnerability without upgrading by adding abort(404) to the very first line of finishSetup in SetupController.php. CVE ID : CVE-2021-21276		
pryaniki					
pryaniki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Feb-21	3.5	A cross-site scripting (XSS) vulnerability in Pryaniki 6.44.3 allows remote authenticated users to upload an arbitrary file. The JavaScript code will execute when someone visits the attachment. CVE ID : CVE-2021-3395	https://pryaniky.com/en/home/	A-PRY-PRYA-160221/244
qa-themes					
q2a_ultimate_seo					
Improper Neutralization of Input During Web Page Generation ('Cross-site	05-Feb-21	3.5	Question2Answer Q2A Ultimate SEO Version 1.3 is affected by cross-site scripting (XSS), which may lead to arbitrary remote code execution. CVE ID : CVE-2021-3258	https://github.com/q2a-projects/Q2A-Ultimate-SEO/commit/20069f28147c6f2c3acca4	A-QA--Q2A_-160221/245

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				e3f6f5154537c5d536, https://www.question2answer.org/qa/58520/important-q2a-ultimate-seo-important-update	

redwood

report2web

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Feb-21	4.3	A cross-site scripting (XSS) issue in the login panel in Redwood Report2Web 4.3.4.5 and 4.5.3 allows remote attackers to inject JavaScript via the signIn.do url parameter. CVE ID : CVE-2021-26710	N/A	A-RED-REPO-160221/246
Externally Controlled Reference to a Resource in Another Sphere	05-Feb-21	5	A frame-injection issue in the online help in Redwood Report2Web 4.3.4.5 allows remote attackers to render an external resource inside a frame via the help/Online_Help/NetHelp/default.htm turl parameter. CVE ID : CVE-2021-26711	N/A	A-RED-REPO-160221/247

Roundcube

roundcube

Improper Neutralization of Input During Web Page Generation ('Cross-site	09-Feb-21	3.5	Roundcube before 1.4.11 allows XSS via crafted Cascading Style Sheets (CSS) token sequences during HTML email rendering. CVE ID : CVE-2021-26925	https://github.com/roundcube/roundcube/commit/9dc276d5f26042db02754fa1bac6f	A-ROU-ROUN-160221/248
--	-----------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				bd683c6d596	
sencha					
connect					
Not Available	03-Feb-21	2.1	<p>This affects all versions of package com.squareup:connect. The method prepareDownloadFile creates a temporary file with the permissions bits of -rw-r--r-- on unix-like systems. On unix-like systems, the system temporary directory is shared between users. As such, the contents of the file downloaded by downloadFileFromResponse will be visible to all other users on the local system. A workaround fix for this issue is to set the system property java.io.tmpdir to a safe directory as remediation. Note: This version of the SDK is end of life and no longer maintained, please upgrade to the latest version.</p> <p>CVE ID : CVE-2021-23331</p>	<p>https://github.com/square/connect-java-sdk/blob/master/src/main/java/com/squareup/connect/ApiClient.java%23L613, https://snyk.io/vuln/SNYK-JAVA-COMSQWAREUP-1065988</p>	A-SEN-CONN-160221/249
set-or-get_project					
set-or-get					
Not Available	08-Feb-21	7.5	<p>Prototype pollution vulnerability in 'set-or-get' version 1.0.0 through 1.2.10 allows an attacker to cause a denial of service and may lead to remote code execution.</p>	<p>https://github.com/IonicaBizau/set-or-get.js/commit/82ede5ccb2e8d13e4f62599203a43</p>	A-SET-SET--160221/250

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25913	89f6d8e936	
Siemens					
cscope					
Out-of-bounds Read	09-Feb-21	6.8	Cscope (All versions prior to 9.90 SP3.5) lacks proper validation of user-supplied data when parsing project files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute code in the context of the current process. CVE ID : CVE-2021-22663	N/A	A-SIE-CSCA-160221/251
smartfoxserver					
smartfoxserver					
Cleartext Storage of Sensitive Information	09-Feb-21	2.1	An issue was discovered in SmartFoxServer 2.17.0. Cleartext password disclosure can occur via /config/server.xml. CVE ID : CVE-2021-26550	N/A	A-SMA-SMAR-160221/252
Solarwinds					
serv-u					
Insecure Storage of Sensitive Information	03-Feb-21	3.6	In SolarWinds Serv-U before 15.2.2 Hotfix 1, there is a directory containing user profile files (that include users' password hashes) that is world readable and writable. An unprivileged Windows user (having access to the server's filesystem) can add an FTP user by copying a valid profile file to this directory. For example, if this profile sets up a user with a	N/A	A-SOL-SERV-160221/253

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C:\ home directory, then the attacker obtains access to read or replace arbitrary files with LocalSystem privileges. CVE ID : CVE-2021-25276		
orion_platform					
Deserializati n of Untrusted Data	03-Feb-21	10	The Collector Service in SolarWinds Orion Platform before 2020.2.4 uses MSMQ (Microsoft Message Queue) and doesn't set permissions on its private queues. As a result, remote unauthenticated clients can send messages to TCP port 1801 that the Collector Service will process. Additionally, upon processing of such messages, the service deserializes them in insecure manner, allowing remote arbitrary code execution as LocalSystem. CVE ID : CVE-2021-25274	https://www.trustwave.com/en-us/resources/blogs/spide-rlabs-blog/full-system-control-with-new-solarwinds-orion-based-and-serv-u-ftp-vulnerabilitie-s/	A-SOL-ORIO-160221/254
Use of Hard- coded Credentials	03-Feb-21	2.1	SolarWinds Orion Platform before 2020.2.4, as used by various SolarWinds products, installs and uses a SQL Server backend, and stores database credentials to access this backend in a file readable by unprivileged users. As a result, any user having access to the filesystem can read database login details from that file, including the login name and its associated password. Then, the credentials can be used to get	N/A	A-SOL-ORIO-160221/255

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>database owner access to the SWNetPerfMon.DB database. This gives access to the data collected by SolarWinds applications, and leads to admin access to the applications by inserting or changing authentication data stored in the Accounts table of the database.</p> <p>CVE ID : CVE-2021-25275</p>		
Sonicwall					
sma_500v					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	<p>A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x.</p> <p>CVE ID : CVE-2021-20016</p>	<p>https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001</p>	A-SON-SMA_-160221/256
sthttpd_project					
sthttpd					
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-Feb-21	5	<p>An issue was discovered in sthttpd through 2.27.1. On systems where the strcpy function is implemented with memcpy, the de_dotdot function may cause a Denial-of-Service (daemon crash) due to overlapping memory ranges being passed to memcpy. This can triggered with an HTTP GET request for a crafted filename. NOTE:</p>	N/A	A-STH-STHT-160221/257

CVSS Scoring Scale	0-1	1-2	2-3	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 is similar to CVE-2017-10671, but occurs in a different part of the de_dotdot function. CVE ID : CVE-2021-26843		
Telegram					
telegram					
Cleartext Storage of Sensitive Information	12-Feb-21	2.1	Telegram before 7.4 (212543) Stable on macOS stores the local passcode in cleartext, leading to information disclosure. CVE ID : CVE-2021-27204	N/A	A-TEL-TELE-160221/258
Cleartext Storage of Sensitive Information	12-Feb-21	2.1	Telegram before 7.4 (212543) Stable on macOS stores the local copy of self-destructed messages in a sandbox path, leading to sensitive information disclosure. CVE ID : CVE-2021-27205	N/A	A-TEL-TELE-160221/259
Tibco					
ebx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Feb-21	6	The TIBCO EBX Web Server component of TIBCO Software Inc.'s TIBCO EBX contains a vulnerability that theoretically allows a low privileged attacker with network access to execute a Stored Cross Site Scripting (XSS) attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 5.9.12 and below. CVE ID : CVE-2021-23271	http://www.tibco.com/services/support/advisories , https://www.tibco.com/support/advisories/2021/02/tibco-security-advisory-february-2-2021-tibco-ebx	A-TIB-EBX-160221/260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
traccar										
traccar										
Unquoted Search Path or Element	02-Feb-21	1.9	Traccar is an open source GPS tracking system. In Traccar before version 4.12 there is an unquoted Windows binary path vulnerability. Only Windows versions are impacted. Attacker needs write access to the filesystem on the host machine. If Java path includes a space, then attacker can lift their privilege to the same as Traccar service (system). This is fixed in version 4.12. CVE ID : CVE-2021-21292	https://github.com/traccar/traccar/commit/cc69a9907ac9878db3750aa14ffedb28626455da , https://github.com/traccar/traccar/security/advisories/GHSA-j75r-7qm5-62q5	A-TRA-TRAC-160221/261					
Trendmicro										
antivirus										
Uncontrolled Resource Consumption	04-Feb-21	1.9	Trend Micro Antivirus for Mac 2021 (Consumer) is vulnerable to a memory exhaustion vulnerability that could lead to disabling all the scanning functionality within the application. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability - i.e. the attacker must already have access to the target system (either legitimately or via another exploit). CVE ID : CVE-2021-25227	https://helpcenter.trendmicro.com/en-us/article/TMKA-10191	A-TRE-ANTI-160221/262					
apex_one										
Incorrect	04-Feb-21	5	An improper access control	https://succe	A-TRE-APEX-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about hotfix history. CVE ID : CVE-2021-25228	ss.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	160221/263
Incorrect Authorization	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the database server. CVE ID : CVE-2021-25229	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	A-TRE-APEX-160221/264
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the contents of a scan connection exception file. CVE ID : CVE-2021-25230	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	A-TRE-APEX-160221/265
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an	https://success.trendmicro.com/solution/000284202 , https://succe	A-TRE-APEX-160221/266

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to obtain information about a specific hotfix history file. CVE ID : CVE-2021-25231	ss.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the SQL database. CVE ID : CVE-2021-25232	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	A-TRE-APEX-160221/267
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific configuration download file. CVE ID : CVE-2021-25233	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-APEX-160221/268
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	A-TRE-APEX-160221/269

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to obtain information about a specific notification configuration file. CVE ID : CVE-2021-25234	ss.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about a content inspection configuration file. CVE ID : CVE-2021-25235	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	A-TRE-APEX-160221/270
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem) could allow an unauthenticated user to obtain information about the managing port used by agents. CVE ID : CVE-2021-25237	https://success.trendmicro.com/solution/000284202	A-TRE-APEX-160221/271
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about x86 agent hotfixes. CVE ID : CVE-2021-25239	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284205	A-TRE-APEX-160221/272

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
				on/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain x64 agent hofitx information. CVE ID : CVE-2021-25240	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	A-TRE-APEX-160221/273
Server-Side Request Forgery (SSRF)	04-Feb-21	5	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a sweep. CVE ID : CVE-2021-25241	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284206	A-TRE-APEX-160221/274
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain version and build information. CVE ID : CVE-2021-25242	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/soluti	A-TRE-APEX-160221/275

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
				on/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain patch level information. CVE ID : CVE-2021-25243	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	A-TRE-APEX-160221/276
Incorrect Authorization	04-Feb-21	6.4	An improper access control information disclosure vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG SP1, and Worry-Free Business Security could allow an unauthenticated user to create a bogus agent on an affected server that could be used then make valid configuration queries. CVE ID : CVE-2021-25246	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	A-TRE-APEX-160221/277
Out-of-bounds Read	04-Feb-21	2.1	An out-of-bounds read information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow an attacker to disclose	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/soluti	A-TRE-APEX-160221/278

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information about a named pipe. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25248	on/000284205, https://success.trendmicro.com/solution/000284206	
Out-of-bounds Write	04-Feb-21	7.2	An out-of-bounds write information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25249	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-APEX-160221/279
officescan					
Incorrect Authorization	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about hotfix history. CVE ID : CVE-2021-25228	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/280

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				06	
Incorrect Authorization	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the database server. CVE ID : CVE-2021-25229	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	A-TRE-OFFI-160221/281
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the contents of a scan connection exception file. CVE ID : CVE-2021-25230	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	A-TRE-OFFI-160221/282
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific hotfix history file. CVE ID : CVE-2021-25231	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/283
Exposure of Sensitive Information to an	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could	https://success.trendmicro.com/solution/0002842	A-TRE-OFFI-160221/284

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			allow an unauthenticated user to obtain information about the SQL database. CVE ID : CVE-2021-25232	02, https://success.trendmicro.com/solution/000284205	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific configuration download file. CVE ID : CVE-2021-25233	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/285
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific notification configuration file. CVE ID : CVE-2021-25234	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/286
Exposure of Sensitive Information to an	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could	https://success.trendmicro.com/solution/0002842	A-TRE-OFFI-160221/287

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			allow an unauthenticated user to obtain information about a content inspection configuration file. CVE ID : CVE-2021-25235	02, https://success.trendmicro.com/solution/000284205	
Server-Side Request Forgery (SSRF)	04-Feb-21	5	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a specific sweep. CVE ID : CVE-2021-25236	https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/288
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about an agent's managing port. CVE ID : CVE-2021-25238	https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/289
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about x86 agent hotfixes. CVE ID : CVE-2021-25239	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/290

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				on/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain x64 agent hofitx information. CVE ID : CVE-2021-25240	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/291
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain version and build information. CVE ID : CVE-2021-25242	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/292
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain patch level	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/soluti	A-TRE-OFFI-160221/293

CVSS Scoring Scale	0-1	1-2	2-3	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. CVE ID : CVE-2021-25243	on/000284205, https://success.trendmicro.com/solution/000284206	
Incorrect Authorization	04-Feb-21	6.4	An improper access control information disclosure vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG SP1, and Worry-Free Business Security could allow an unauthenticated user to create a bogus agent on an affected server that could be used then make valid configuration queries. CVE ID : CVE-2021-25246	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/294
Out-of-bounds Read	04-Feb-21	2.1	An out-of-bounds read information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow an attacker to disclose sensitive information about a named pipe. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25248	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-160221/295
Out-of-	04-Feb-21	7.2	An out-of-bounds write information disclosure	https://success.trendmicro.com/solution/000284206	A-TRE-OFFI-

CVSS Scoring Scale	0-1	1-2	2-3	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 Write			vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25249	o.com/solution/000284202, https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	160221/296

worry-free_business_security

Incorrect Authorization	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about hotfix history. CVE ID : CVE-2021-25228	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/297
-------------------------	-----------	---	---	---	-----------------------

Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific hotfix history file.	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 ,	A-TRE-WORR-160221/298
--	-----------	---	---	--	-----------------------

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25231	https://success.trendmicro.com/solution/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific configuration download file. CVE ID : CVE-2021-25233	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/299
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific notification configuration file. CVE ID : CVE-2021-25234	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/300
Server-Side Request Forgery (SSRF)	04-Feb-21	5	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business	https://success.trendmicro.com/solution/000284205 ,	A-TRE-WORR-160221/301

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a specific sweep. CVE ID : CVE-2021-25236	https://success.trendmicro.com/solution/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about an agent's managing port. CVE ID : CVE-2021-25238	https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/302
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about x86 agent hotfixes. CVE ID : CVE-2021-25239	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/303
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain x64 agent hofitx information.	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/304

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25240	05, https://success.trendmicro.com/solution/000284206	
Server-Side Request Forgery (SSRF)	04-Feb-21	5	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a sweep. CVE ID : CVE-2021-25241	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/305
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain version and build information. CVE ID : CVE-2021-25242	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/306
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain patch level	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/307

CVSS Scoring Scale	0-1	1-2	2-3	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. CVE ID : CVE-2021-25243	05, https://success.trendmicro.com/solution/000284206	
Incorrect Authorization	04-Feb-21	5	An improper access control vulnerability in Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain various pieces of configuration information. CVE ID : CVE-2021-25244	https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/308
Incorrect Authorization	04-Feb-21	5	An improper access control vulnerability in Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain various pieces of settings information. CVE ID : CVE-2021-25245	https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/309
Incorrect Authorization	04-Feb-21	6.4	An improper access control information disclosure vulnerability in Trend Micro Apex One, Apex One as a Service, OfficeScan XG SP1, and Worry-Free Business Security could allow an unauthenticated user to create a bogus agent on an affected server that could be used then make valid configuration queries. CVE ID : CVE-2021-25246	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/310
Out-of-bounds Read	04-Feb-21	2.1	An out-of-bounds read information disclosure	https://success.trendmicro.com/solution/000284206	A-TRE-WORR-

CVSS Scoring Scale	0-1	1-2	2-3	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 in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow an attacker to disclose sensitive information about a named pipe. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25248	o.com/solution/000284202, https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	160221/311
Out-of-bounds Write	04-Feb-21	7.2	An out-of-bounds write information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25249	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	A-TRE-WORR-160221/312
typelevel					
blaze					
Uncontrolled Resource Consumption	02-Feb-21	5	blaze is a Scala library for building asynchronous pipelines, with a focus on network IO. All servers running blaze-core before version 0.14.15 are affected by a vulnerability in which	https://github.com/http4s/blaze/commit/4f786177f9fb71ab272f3a5f6c80bca3e5662aa1	A-TYP-BLAZ-160221/313

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unbounded connection acceptance leads to file handle exhaustion. Blaze, accepts connections unconditionally on a dedicated thread pool. This has the net effect of amplifying degradation in services that are unable to handle their current request load, since incoming connections are still accepted and added to an unbounded queue. Each connection allocates a socket handle, which drains a scarce OS resource. This can also confound higher level circuit breakers which work based on detecting failed connections. The vast majority of affected users are using it as part of http4s-blaze-server <= 0.21.16. http4s provides a mechanism for limiting open connections, but is enforced inside the Blaze accept loop, after the connection is accepted and the socket opened. Thus, the limit only prevents the number of connections which can be simultaneously processed, not the number of connections which can be held open. The issue is fixed in version 0.14.15 for "NIO1SocketServerGroup". A "maxConnections" parameter is added, with a default value of 512. Concurrent</p>	, https://github.com/http4s/blaze/security/advisories/GHSA-xmw9-q7x9-j5qc	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connections beyond this limit are rejected. To run unbounded, which is not recommended, set a negative number. The "NIO2SocketServerGroup" has no such setting and is now deprecated. There are several possible workarounds described in the referenced GitHub Advisory GHSA-xmw9-q7x9-j5qc. CVE ID : CVE-2021-21293		

http4s

Uncontrolled Resource Consumption	02-Feb-21	5	Http4s (http4s-blaze-server) is a minimal, idiomatic Scala interface for HTTP services. Http4s before versions 0.21.17, 0.22.0-M2, and 1.0.0-M14 have a vulnerability which can lead to a denial-of-service. Blaze-core, a library underlying http4s-blaze-server, accepts connections unboundedly on its selector pool. This has the net effect of amplifying degradation in services that are unable to handle their current request load, since incoming connections are still accepted and added to an unbounded queue. Each connection allocates a socket handle, which drains a scarce OS resource. This can also confound higher level circuit breakers which work based on detecting failed	https://github.com/http4s/http4s/commit/987d6589ef79545b9bb2324ac4deb82d9a0171 , https://github.com/http4s/http4s/security/advisories/GHSA-xhv5-w9c5-2r2w	A-TYP-HTTP-160221/314
-----------------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>connections. http4s provides a general "MaxActiveRequests" middleware mechanism for limiting open connections, but it is enforced inside the Blaze accept loop, after the connection is accepted and the socket opened. Thus, the limit only prevents the number of connections which can be simultaneously processed, not the number of connections which can be held open. In 0.21.17, 0.22.0-M2, and 1.0.0-M14, a new "maxConnections" property, with a default value of 1024, has been added to the `BlazeServerBuilder`. Setting the value to a negative number restores unbounded behavior, but is strongly disrecommended. The NIO2 backend does not respect `maxConnections`. Its use is now deprecated in http4s-0.21, and the option is removed altogether starting in http4s-0.22. There are several possible workarounds described in the referenced GitHub Advisory GHSA-xhv5-w9c5-2r2w.</p> <p>CVE ID : CVE-2021-21294</p>		

wikindx_project

wikindx

Improper Neutralizatio	01-Feb-21	4.3	A cross-site scripting (XSS) vulnerability in many forms	N/A	A-WIK-WIKI-
------------------------	-----------	-----	--	-----	-------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			of Wikindx before 5.7.0 and 6.x through 6.4.0 allows remote attackers to inject arbitrary web script or HTML via the message parameter to index.php?action=initLogon or modules/admin/DELETEIMAGES.php. CVE ID : CVE-2021-3340		160221/315

Wpdatatables

wpdatatables

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Feb-21	10	wpDataTables before 3.4.1 mishandles order direction for server-side tables, aka admin-ajax.php?action=get_wdtable_order[0][dir] SQL injection. CVE ID : CVE-2021-26754	https://wpdatatables.com/help/whats-new-changelog/	A-WPD-WPDA-160221/316
--	-----------	----	---	---	-----------------------

wwbn

avideo

Incorrect Authorization	01-Feb-21	6.5	AVideo Platform is an open-source Audio and Video platform. It is similar to a self-hosted YouTube. In AVideo Platform before version 10.2 there is an authorization bypass vulnerability which enables an ordinary user to get admin control. This is fixed in version 10.2. All queries now remove the pass hash and the recoverPass hash. CVE ID : CVE-2021-21286	https://avideo.tube/ , https://github.com/WWBN/AVideo/security/advisories/GHSA-xq8j-fhg5-hr39	A-WWB-AVID-160221/317
-------------------------	-----------	-----	--	--	-----------------------

Operating System

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Apple					
mac_os					
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21035	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/318
Integer Overflow or Wraparound	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Integer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21036	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/319
Improper Limitation of	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074	https://helpx.adobe.com/s	O-APP-MAC_-160221/320

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			(and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Path Traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21037	security/products/acrobat/apsb21-09.html	
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21038	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/321
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use	https://helpx.adobe.com/security/products/acrobat/apsb21-	O-APP-MAC_-160221/322

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
			After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21039	09.html	
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21040	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/323
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/324

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21041		
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally escalate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21042	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/325
Out-of-bounds Write	11-Feb-21	9.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/326

CVSS Scoring Scale	0-1	1-2	2-3	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 open a malicious file. CVE ID : CVE-2021-21044		
Improper Access Control	11-Feb-21	9.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper access control vulnerability. An unauthenticated attacker could leverage this vulnerability to elevate privileges in the context of the current user. CVE ID : CVE-2021-21045	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/327
Access of Memory Location After End of Buffer	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21046	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/328
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/329

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21017		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21021	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/330
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/331

CVSS Scoring Scale	0-1	1-2	2-3	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 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21028		
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21033	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/332
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally elevate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/333

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. CVE ID : CVE-2021-21034		
NULL Pointer Dereference	11-Feb-21	4.3	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a null pointer dereference vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve denial of service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21057	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/334
Improper Input Validation	11-Feb-21	4.3	Adobe Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21060	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/335

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
Use After Free	11-Feb-21	4.3	Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use-after-free vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21061	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-APP-MAC_-160221/336
Use After Free	09-Feb-21	6.8	Use after free in Payments in Google Chrome on Mac prior to 88.0.4324.146 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21142	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	O-APP-MAC_-160221/337
Cleartext Storage of Sensitive Information	12-Feb-21	2.1	Telegram before 7.4 (212543) Stable on macOS stores the local passcode in cleartext, leading to information disclosure. CVE ID : CVE-2021-27204	N/A	O-APP-MAC_-160221/338
Cleartext Storage of Sensitive Information	12-Feb-21	2.1	Telegram before 7.4 (212543) Stable on macOS stores the local copy of self-destructed messages in a sandbox path, leading to sensitive information disclosure.	N/A	O-APP-MAC_-160221/339

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-27205		
iphone_os					
Authentication Bypass by Spoofing	09-Feb-21	4.3	Incorrect security UI in Page Info in Google Chrome on iOS prior to 88.0.4324.96 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-21134	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	O-APP-IPHO-160221/340
Asus					
rt-ax3000_firmware					
Not Available	05-Feb-21	7.8	Denial of service in ASUSWRT ASUS RT-AX3000 firmware versions 3.0.0.4.384_10177 and earlier versions allows an attacker to disrupt the use of device setup services via continuous login error. CVE ID : CVE-2021-3229	https://dlcdnimgs.asus.com/websites/global/productcustomizedTab/562/ASUSWRT%20portal%20feature.pdf , https://www.asus.com/us/ASUSWRT/	O-ASU-RT-A-160221/341
Belkin					
linksys_wrt160nl_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Feb-21	9	** UNSUPPORTED WHEN ASSIGNED ** The administration web interface on Belkin Linksys WRT160NL 1.0.04.002_US_20130619 devices allows remote authenticated attackers to execute system commands with root privileges via shell metacharacters in the ui_language POST parameter	N/A	O-BEL-LINK-160221/342

CVSS Scoring Scale	0-1	1-2	2-3	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 the apply.cgi form endpoint. This occurs in do_upgrade_post in mini_httpd. NOTE: This vulnerability only affects products that are no longer supported by the maintainer CVE ID : CVE-2021-25310		

Cisco

rv160w_wireless-ac_vpn_router_firmware

External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/343
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV16-160221/344

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1290</p>	sa-rv160-260-rce-XZeFkNHf	
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1291</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	O-CIS-RV16-160221/345

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1292	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/346
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/347

CVSS Scoring Scale	0-1	1-2	2-3	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 of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1293		
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1294	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/348
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/349

CVSS Scoring Scale	0-1	1-2	2-3	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 HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1295		
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1296	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV16-160221/350
Absolute Path	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-RV16-160221/351

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal			Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297	/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	

rv260_vpn_router_firmware

External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/352
---	-----------	----	---	---	-----------------------

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
			interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289		
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1290	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/353
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/354

CVSS Scoring Scale	0-1	1-2	2-3	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 HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1291		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1292	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/355
External Control of Assumed-Immutable Web	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/356

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Parameter			<p>RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1293</p>	visory/cisco-sa-rv160-260-rce-XZeFkNHf	
Not Available	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	O-CIS-RV26-160221/357

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1294		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1295	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/358
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV26-160221/359

CVSS Scoring Scale	0-1	1-2	2-3	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 web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1296		
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV26-160221/360
rv260p_vpn_router_with_poe_firmware					
External Control of Assumed-Immutable	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV26-160221/361

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Parameter			RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289	coSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/362

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code on the device. CVE ID : CVE-2021-1290		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1291	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/363
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/364

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1292		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1293	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/365
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-	O-CIS-RV26-160221/366

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1294</p>	XZeFkNHf	
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1295</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/367
Absolute Path	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small</p>	https://tools.cisco.com/security/center	O-CIS-RV26-160221/368

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal			Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1296	/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV26-160221/369

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297		
rv260w_wireless-ac_vpn_router_firmware					
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/370
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-	O-CIS-RV26-160221/371

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1290</p>	XZeFkNHf	
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1291</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	O-CIS-RV26-160221/372
External Control of	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management</p>	<p>https://tools.cisco.com/se</p>	O-CIS-RV26-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assumed-Immutable Web Parameter			<p>interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1292</p>	<p>curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	160221/373
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	O-CIS-RV26-160221/374

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1293		
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1294	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/375
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV26-160221/376

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1295		
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1296	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV26-160221/377
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV26-160221/378

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297	visory/cisco-sa-rv160-260-filewrite-7x9mnKjn	

rv160_vpn_router_firmware

External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/379
---	-----------	----	---	---	-----------------------

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
			could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289		
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1290	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/380
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/381

CVSS Scoring Scale	0-1	1-2	2-3	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 exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1291		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1292	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/382
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-	O-CIS-RV16-160221/383

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
			<p>remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1293</p>	260-rce-XZeFkNHf	
Not Available	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1294</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	O-CIS-RV16-160221/384

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1295	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	O-CIS-RV16-160221/385
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV16-160221/386

CVSS Scoring Scale	0-1	1-2	2-3	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 to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1296		
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	O-CIS-RV16-160221/387
rv016_multi-wan_vpn_router_firmware					
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv016-042-042g-082-320-filewrite-7x9mnKjn	O-CIS-RV01-160221/388

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1334</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/389

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
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/390

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/391

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1337		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1338	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/392
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/393

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/394

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/395

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1341</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/396

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
			administrator credentials on the affected device. CVE ID : CVE-2021-1342		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1343	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/397
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/398

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/399

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
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/400

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1346</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/401

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1347		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/402
Improper Neutralization of Special Elements used in a	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/403

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			<p>RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1314</p>	visory/cisco-sa-rv-command-inject-BY4c5zd	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV01-160221/404

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
			<p>sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1315</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV01-160221/405

CVSS Scoring Scale	0-1	1-2	2-3	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. CVE ID : CVE-2021-1316		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1317	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV01-160221/406
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-	O-CIS-RV01-160221/407

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1318</p>	BY4c5zd	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/408

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1319		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/409

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1320		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/410
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV01-160221/411

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1322</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/412

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/413

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/414

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1325		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/415
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV01-160221/416

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1327</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/417

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV01-160221/418

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1329		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/419

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1330		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/420
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV01-160221/421

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1332</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV01-160221/422

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
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1333</p>		

rv042_dual_wan_vpn_router_firmware

Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/423
-----------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1334</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/424

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1335		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1336	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/425
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-RV04-160221/426

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/427

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1338</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV04-160221/428

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/429

CVSS Scoring Scale	0-1	1-2	2-3	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, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1340		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1341	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/430
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-RV04-160221/431

CVSS Scoring Scale	0-1	1-2	2-3	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			Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1342	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/432

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1343</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/433

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/434

CVSS Scoring Scale	0-1	1-2	2-3	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, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1345		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1346	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/435
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-RV04-160221/436

CVSS Scoring Scale	0-1	1-2	2-3	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			Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1347	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/437

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1348</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	0-CIS-RV04-160221/438

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1314</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1315</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV04-160221/439

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1316	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV04-160221/440
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV04-160221/441

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1317</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV04-160221/442

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1319	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/443

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/444
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV04-160221/445

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
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/446

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1322</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV04-160221/447

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
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/448

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/449
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	O-CIS-RV04-160221/450

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/451

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1327</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV04-160221/452

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
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/453

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/454
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	O-CIS-RV04-160221/455

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/456

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1332</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV04-160221/457

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1333</p>		
rv042g_dual_gigabit_wan_vpn_router_firmware					
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/458

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1334		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/459
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV04-160221/460

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>	overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/461

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/462

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1338		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/463

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
			CVE ID : CVE-2021-1339		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/464
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV04-160221/465

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1341</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/466

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1342</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/467

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1343		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/468

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
			CVE ID : CVE-2021-1344		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/469
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV04-160221/470

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1346</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/471

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
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1347</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/472

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1314	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV04-160221/473
Improper Neutralization	04-Feb-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	O-CIS-RV04-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315	curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	160221/474
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV04-160221/475

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1316</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	0-CIS-RV04-160221/476

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
			attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1317		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV04-160221/477
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV04-160221/478

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/479

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/480

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1321</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/481

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1322		
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1323	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/482
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV04-160221/483

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/484

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/485

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1326</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/486

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1327		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1328	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/487
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV04-160221/488

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/489

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
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/490

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1331</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV04-160221/491

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1332		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1333	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV04-160221/492
rv082_dual_wan_vpn_router_firmware					
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV08-160221/493

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1334</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/494

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/495

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
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/496

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1337		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1338	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/497
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV08-160221/498

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/499

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/500

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1341</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/501

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1342		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1343	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/502
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV08-160221/503

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/505

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
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1346</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/506

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
			would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1347		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/507
Improper Neutralization of Special Elements	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	O-CIS-RV08-160221/508

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
used in a Command ('Command Injection')			RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1314	coSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV08-160221/509

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1315</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV08-160221/510

CVSS Scoring Scale	0-1	1-2	2-3	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 on an affected device. CVE ID : CVE-2021-1316		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1317	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV08-160221/511
Improper Neutralization of Special Elements used in a Command ('Command	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-	O-CIS-RV08-160221/512

CVSS Scoring Scale	0-1	1-2	2-3	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')			<p>commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1318</p>	inject-BY4c5zd	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/513

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/514

CVSS Scoring Scale	0-1	1-2	2-3	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, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1320		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/515
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-RV08-160221/516

CVSS Scoring Scale	0-1	1-2	2-3	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			<p>Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1322</p>	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/517

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
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV08-160221/518

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/519

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
			vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1325		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/520
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-RV08-160221/521

CVSS Scoring Scale	0-1	1-2	2-3	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			Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1327	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/522

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
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/523

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV08-160221/524

CVSS Scoring Scale	0-1	1-2	2-3	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, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1330		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/525
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-RV08-160221/526

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
Overflow			<p>Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1332</p>	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV08-160221/527

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1333</p>		

rv320_dual_gigabit_wan_vpn_router_firmware

Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/528
-----------------------------	-----------	---	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1334</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS)</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/529

CVSS Scoring Scale	0-1	1-2	2-3	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. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1335		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1336	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/530
Out-of-	04-Feb-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	O-CIS-RV32-

CVSS Scoring Scale	0-1	1-2	2-3	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 Write			<p>interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>	curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	160221/531
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/532

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1338</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/533

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
			<p>requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS)</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/534

CVSS Scoring Scale	0-1	1-2	2-3	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. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1340		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1341	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/535
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	O-CIS-RV32-

CVSS Scoring Scale	0-1	1-2	2-3	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			<p>interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1342</p>	curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	160221/536
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/537

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
			<p>unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1343</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/538

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1344		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/539

CVSS Scoring Scale	0-1	1-2	2-3	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. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1345		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1346	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/540
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	O-CIS-RV32-

CVSS Scoring Scale	0-1	1-2	2-3	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			<p>interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1347</p>	curoty/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	160221/541
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/542

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1348</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV32-160221/543

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1314</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1315</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV32-160221/544

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
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1316	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV32-160221/545
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV32-160221/546

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1317</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	O-CIS-RV32-160221/547

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
			operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1319	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/548

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/549
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV32-160221/550

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/551

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1322</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/552

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
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/553

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/554
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	O-CIS-RV32-160221/555

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/556

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1327</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/557

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
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/558

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/559
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	0-CIS-RV32-160221/560

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/561

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1332</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/562

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1333</p>		
rv325_dual_gigabit_wan_vpn_router_firmware					
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/563

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1334		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/564
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV32-160221/565

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
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>	overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/566

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/567

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1338		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/568

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1339		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/569
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-</p>	O-CIS-RV32-160221/570

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1341</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/571

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1342</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/572

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
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1343		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/573

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1344		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/574
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-</p>	O-CIS-RV32-160221/575

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1346</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/576

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
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1347</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/577

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1314	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV32-160221/578
Improper Neutralization	04-Feb-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	O-CIS-RV32-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315	curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	160221/579
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV32-160221/580

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
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1316</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	0-CIS-RV32-160221/581

CVSS Scoring Scale	0-1	1-2	2-3	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 would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1317		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	O-CIS-RV32-160221/582
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV32-160221/583

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/584

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/585

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1321</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/586

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1322		
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1323	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/587
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV32-160221/588

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
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/589

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/590

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1326</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/591

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
			the affected device. CVE ID : CVE-2021-1327		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1328	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/592
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-RV32-160221/593

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/594

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	O-CIS-RV32-160221/595

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1331</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	0-CIS-RV32-160221/596

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1332		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1333	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	O-CIS-RV32-160221/597
nx-os					
Improper Access Control	04-Feb-21	6.4	A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco	https://tools.cisco.com/security/center/content/Cis	O-CIS-NX-O-160221/598

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.</p> <p>CVE ID : CVE-2021-1389</p>	coSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j	

ios_xr

Improper Access Control	04-Feb-21	5	<p>A vulnerability in the Local Packet Transport Services (LPTS) programming of the SNMP with the management plane protection feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to allow connections despite the management plane protection that is configured to deny access to the SNMP server of an affected device. This vulnerability is due to incorrect LPTS programming when using SNMP with management plane protection. An attacker could exploit this vulnerability by</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-7MKrW7Nq</p>	O-CIS-IOS_-160221/599
-------------------------	-----------	---	---	--	-----------------------

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
			connecting to an affected device using SNMP. A successful exploit could allow the attacker to connect to the device on the configured SNMP ports. Valid credentials are required to execute any of the SNMP requests. CVE ID : CVE-2021-1243		
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1244	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	O-CIS-IOS_-160221/600
Not Available	04-Feb-21	7.8	Multiple vulnerabilities in the ingress packet processing function of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1288	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dos-WwDdghs2	O-CIS-IOS_-160221/601
Insertion of Sensitive	04-Feb-21	2.1	A vulnerability in the CLI parser of Cisco IOS XR	https://tools.cisco.com/se	O-CIS-IOS_-160221/602

CVSS Scoring Scale	0-1	1-2	2-3	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 Into Sent Data			Software could allow an authenticated, local attacker to view more information than their privileges allow. The vulnerability is due to insufficient application of restrictions during the execution of a specific command. An attacker could exploit this vulnerability by using a specific command at the command line. A successful exploit could allow the attacker to obtain sensitive information within the configuration that otherwise might not have been accessible beyond the privileges of the invoking user. CVE ID : CVE-2021-1128	curity/center/content/CiscoSecurityAdvisory/cisco-sa-ios-infodisc-4mtm9Gyt	
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1136	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-lzNhcGCBt	O-CIS-IOS_-160221/603
Insufficient Adherence to Expected	04-Feb-21	3.3	A vulnerability in the IPv6 protocol handling of the management interfaces of	https://tools.cisco.com/security/center	O-CIS-IOS_-160221/604

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conventions			<p>Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause an IPv6 flood on the management interface network of an affected device. The vulnerability exists because the software incorrectly forwards IPv6 packets that have an IPv6 node-local multicast group address destination and are received on the management interfaces. An attacker could exploit this vulnerability by connecting to the same network as the management interfaces and injecting IPv6 packets that have an IPv6 node-local multicast group address destination. A successful exploit could allow the attacker to cause an IPv6 flood on the corresponding network. Depending on the number of Cisco IOS XR Software nodes on that network segment, exploitation could cause excessive network traffic, resulting in network degradation or a denial of service (DoS) condition.</p> <p>CVE ID : CVE-2021-1268</p>	/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K	
Not Available	04-Feb-21	7.8	<p>Multiple vulnerabilities in the ingress packet processing function of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	0-CIS-IOS_-160221/605

CVSS Scoring Scale	0-1	1-2	2-3	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 (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1313	sa-iosxr-dos-WwDdghs2	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-21	7.2	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running NCS540L software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device. The vulnerability is due to insufficient validation of command line arguments. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level privileges to escalate their privilege level to root. CVE ID : CVE-2021-1370	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pe-QpzCAePe	O-CIS-IOS_-160221/606
Improper Access Control	04-Feb-21	6.4	A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-	O-CIS-IOS_-160221/607

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
			<p>is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.</p> <p>CVE ID : CVE-2021-1389</p>	CHgdYk8j	

Dell

emc_powerscale_onefs

Improper Privilege Management	09-Feb-21	7.5	<p>Dell PowerScale OneFS versions 8.1.0 – 9.1.0 contain a "use of SSH key past account expiration" vulnerability. A user on the network with the ISI_PRIV_AUTH_SSH RBAC privilege that has an expired account may potentially exploit this vulnerability, giving them access to the same things they had before account expiration. This may be by a high privileged account and hence Dell recommends customers upgrade at the earliest opportunity.</p> <p>CVE ID : CVE-2021-21502</p>	<p>https://www.dell.com/support/kbdoc/en-us/000182873/dsa-2021-009-dell-powerscale-onefs-security-update-for-multiple-vulnerabilities</p>	O-DEL-EMC_-160221/608
-------------------------------	-----------	-----	---	--	-----------------------

elecom

wrc-300febka_firmware

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Feb-21	4.3	Cross-site scripting vulnerability in ELECOM WRC-300FEBK-A allows remote authenticated attackers to inject arbitrary script via unspecified vectors. CVE ID : CVE-2021-20645	https://www.elecom.co.jp/news/security/20210126-01/	O-ELE-WRC--160221/609
Cross-Site Request Forgery (CSRF)	12-Feb-21	4.3	Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-A allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started. CVE ID : CVE-2021-20646	https://www.elecom.co.jp/news/security/20210126-01/	O-ELE-WRC--160221/610
wrc-300febk-s_firmware					
Cross-Site Request Forgery (CSRF)	12-Feb-21	4.3	Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-S allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started. CVE ID : CVE-2021-20647	https://www.elecom.co.jp/news/security/20210126-01/	O-ELE-WRC--160221/611
Improper Neutralization of Special Elements used in an OS Command	12-Feb-21	7.7	ELECOM WRC-300FEBK-S allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors.	https://www.elecom.co.jp/news/security/20210126-01/	O-ELE-WRC--160221/612

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			CVE ID : CVE-2021-20648		
Improper Certificate Validation	12-Feb-21	5.8	ELECOM WRC-300FEBK-S contains an improper certificate validation vulnerability. Via a man-in-the-middle attack, an attacker may alter the communication response. As a result, an arbitrary OS command may be executed on the affected device. CVE ID : CVE-2021-20649	https://www.elecom.co.jp/news/security/20210126-01/	O-ELE-WRC--160221/613
Fedoraproject					
fedora					
Use After Free	09-Feb-21	6.8	Use after free in Payments in Google Chrome on Mac prior to 88.0.4324.146 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21142	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	O-FED-FEDO-160221/614
Out-of-bounds Write	09-Feb-21	6.8	Heap buffer overflow in Extensions in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. CVE ID : CVE-2021-21143	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	O-FED-FEDO-160221/615
Out-of-bounds Write	09-Feb-21	6.8	Heap buffer overflow in Tab Groups in Google Chrome prior to 88.0.4324.146 allowed an attacker who	https://chromereleases.googleblog.com/2021/02/	O-FED-FEDO-160221/616

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. CVE ID : CVE-2021-21144	stable-channel-update-for-desktop.html, https://crbug.com/1163845	
Use After Free	09-Feb-21	6.8	Use after free in Fonts in Google Chrome prior to 88.0.4324.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21145	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	O-FED-FEDO-160221/617
Use After Free	09-Feb-21	6.8	Use after free in Navigation in Google Chrome prior to 88.0.4324.146 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21146	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	O-FED-FEDO-160221/618
Not Available	09-Feb-21	4.3	Inappropriate implementation in Skia in Google Chrome prior to 88.0.4324.146 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. CVE ID : CVE-2021-21147	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	O-FED-FEDO-160221/619
fiberhome					
hg6245d_firmware					
Not Available	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to extract	N/A	O-FIB-HG62-160221/620

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from the device without authentication by disabling JavaScript and visiting /info.asp. CVE ID : CVE-2021-27139		
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to find passwords and authentication cookies stored in cleartext in the web.log HTTP logs. CVE ID : CVE-2021-27140	N/A	O-FIB-HG62-160221/621
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. Credentials in /fhconf/umconfig.txt are obfuscated via XOR with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@\$a2s0i3g key. (The webs binary has details on how XOR is used.) CVE ID : CVE-2021-27141	N/A	O-FIB-HG62-160221/622
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web management is done over HTTPS, using a hardcoded private key that has 0777 permissions. CVE ID : CVE-2021-27142	N/A	O-FIB-HG62-160221/623
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / user1234 credentials for an ISP.	N/A	O-FIB-HG62-160221/624

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-27143		
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded f~!b@e#r\$h%o^m*esuperadmin / s(f)u_h+g u credentials for an ISP. CVE ID : CVE-2021-27144	N/A	O-FIB-HG62-160221/625
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / lnadmin credentials for an ISP. CVE ID : CVE-2021-27145	N/A	O-FIB-HG62-160221/626
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / CUadmin credentials for an ISP. CVE ID : CVE-2021-27146	N/A	O-FIB-HG62-160221/627
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / admin credentials for an ISP. CVE ID : CVE-2021-27147	N/A	O-FIB-HG62-160221/628
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded telecomadmin / nE7jA%5m credentials for an ISP.	N/A	O-FIB-HG62-160221/629

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27148		
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded adminpldt / z6dUABtl270qRxt7a2uGTiw credentials for an ISP. CVE ID : CVE-2021-27149	N/A	O-FIB-HG62-160221/630
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded gestiontelebucaramanga / t3l3buc4r4m4ng42013 credentials for an ISP. CVE ID : CVE-2021-27150	N/A	O-FIB-HG62-160221/631
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded rootmet / m3tr0r00t credentials for an ISP. CVE ID : CVE-2021-27151	N/A	O-FIB-HG62-160221/632
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded awnfibre / fibre@dm!n credentials for an ISP. CVE ID : CVE-2021-27152	N/A	O-FIB-HG62-160221/633
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the	N/A	O-FIB-HG62-160221/634

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					
			hardcoded trueadmin / admintrue credentials for an ISP. CVE ID : CVE-2021-27153							
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / GOR2U1P2ag credentials for an ISP. CVE ID : CVE-2021-27154	N/A	O-FIB-HG62-160221/635					
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 3UJUUh2VemEfUtesEchEC2d2e credentials for an ISP. CVE ID : CVE-2021-27155	N/A	O-FIB-HG62-160221/636					
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains credentials for an ISP that equal the last part of the MAC address of the br0 interface. CVE ID : CVE-2021-27156	N/A	O-FIB-HG62-160221/637					
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 888888 credentials for an ISP. CVE ID : CVE-2021-27157	N/A	O-FIB-HG62-160221/638					
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web	N/A	O-FIB-HG62-160221/639					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			daemon contains the hardcoded L1vt1m4eng / 888888 credentials for an ISP. CVE ID : CVE-2021-27158		
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded useradmin / 888888 credentials for an ISP. CVE ID : CVE-2021-27159	N/A	O-FIB-HG62-160221/640
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / 888888 credentials for an ISP. CVE ID : CVE-2021-27160	N/A	O-FIB-HG62-160221/641
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 1234 credentials for an ISP. CVE ID : CVE-2021-27161	N/A	O-FIB-HG62-160221/642
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / tattoo@home credentials for an ISP. CVE ID : CVE-2021-27162	N/A	O-FIB-HG62-160221/643
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web	N/A	O-FIB-HG62-160221/644

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			daemon contains the hardcoded admin / tele1234 credentials for an ISP. CVE ID : CVE-2021-27163		
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / aisadmin credentials for an ISP. CVE ID : CVE-2021-27164	N/A	O-FIB-HG62-160221/645
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The telnet daemon on port 23/tcp can be abused with the gpon/gpon credentials. CVE ID : CVE-2021-27165	N/A	O-FIB-HG62-160221/646
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The password for the enable command is gpon. CVE ID : CVE-2021-27166	N/A	O-FIB-HG62-160221/647
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a password of four hexadecimal characters for the admin account. These characters are generated in init_3bb_password in libci_adaptation_layer.so. CVE ID : CVE-2021-27167	N/A	O-FIB-HG62-160221/648
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a 6GFjdY4aAuUKjdtSn7d	N/A	O-FIB-HG62-160221/649

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password for the rdsadmin account. CVE ID : CVE-2021-27168		
Insecure Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. By default, there are no firewall rules for IPv6 connectivity, exposing the internal management interfaces to the Internet. CVE ID : CVE-2021-27170	N/A	O-FIB-HG62-160221/650
Out-of-bounds Write	10-Feb-21	10	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to start a Linux telnetd as root on port 26/tcp by using the CLI interface commands of ddd and shell (or tshell). CVE ID : CVE-2021-27171	N/A	O-FIB-HG62-160221/651
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. A hardcoded GEAPON password for root is defined inside /etc/init.d/system-config.sh. CVE ID : CVE-2021-27172	N/A	O-FIB-HG62-160221/652
Improper Authentication	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a telnet?enable=0&key=calculated(BR0_MAC) backdoor API, without authentication, provided by the HTTP server. This will remove firewall rules and allow an attacker to reach the telnet server (used for the CLI).	N/A	O-FIB-HG62-160221/653

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-27173							
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. wifi_custom.cfg has cleartext passwords and 0644 permissions. CVE ID : CVE-2021-27174	N/A	O-FIB-HG62-160221/654					
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_2g.cfg has cleartext passwords and 0644 permissions. CVE ID : CVE-2021-27175	N/A	O-FIB-HG62-160221/655					
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_5g.cfg has cleartext passwords and 0644 permissions. CVE ID : CVE-2021-27176	N/A	O-FIB-HG62-160221/656					
Incorrect Authorization	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to bypass authentication by sending the decoded value of the GgpoZWxwCmxc3QKd2hvcg== string to the telnet server. CVE ID : CVE-2021-27177	N/A	O-FIB-HG62-160221/657					
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. Some passwords are stored in cleartext in nvram. CVE ID : CVE-2021-27178	N/A	O-FIB-HG62-160221/658					
CVSS Scoring Scale	0-1	1-2	2-3	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	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to crash the telnet daemon by sending a certain 0a 65 6e 61 62 6c 65 0a 02 0a 1a 0a string. CVE ID : CVE-2021-27179	N/A	O-FIB-HG62-160221/659
an5506-04-fa_firmware					
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome AN5506-04-FA devices with firmware RP2631. There is a gepon password for the gepon account. CVE ID : CVE-2021-27169	N/A	O-FIB-AN55-160221/660
Google					
android					
Improper Restriction of Rendered UI Layers or Frames	10-Feb-21	6.9	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible overlay attack due to an insecure default value. This could lead to local escalation of privilege and notification access with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-170731783 CVE ID : CVE-2021-0331	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/661
Use After Free	10-Feb-21	7.2	In bootFinished of SurfaceFlinger.cpp, there is a possible memory corruption due to a use after free. This	https://source.android.com/security/bulletin/2021-	O-GOO-ANDR-160221/662

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-169256435 CVE ID : CVE-2021-0332	02-01	
Improper Restriction of Rendered UI Layers or Frames	10-Feb-21	6.9	In onCreate of BluetoothPermissionActivity.java, there is a possible permissions bypass due to a tapjacking overlay that obscures the phonebook permissions dialog when a Bluetooth device is connecting. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-168504491 CVE ID : CVE-2021-0333	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/663
Incorrect Permission Assignment for Critical Resource	10-Feb-21	7.2	In onTargetSelected of ResolverActivity.java, there is a possible settings bypass allowing an app to become the default handler for arbitrary domains. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/664

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-163358811 CVE ID : CVE-2021-0334		
Use After Free	10-Feb-21	4.3	In process of C2SoftHevcDec.cpp, there is a possible out of bounds write due to a use after free. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160346309 CVE ID : CVE-2021-0335	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/665
Improper Privilege Management	10-Feb-21	7.2	In onReceive of BluetoothPermissionRequest.java, there is a possible permissions bypass due to a mutable PendingIntent. This could lead to local escalation of privilege that bypasses a permission check, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-158219161 CVE ID : CVE-2021-0336	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/666
Cleartext Storage of Sensitive Information	10-Feb-21	7.2	In moveInMediaStore of FileSystemProvider.java, there is a possible file exposure due to stale	https://source.android.com/security/bulletin/2021-	O-GOO-ANDR-160221/667

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			metadata. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-157474195 CVE ID : CVE-2021-0337	02-01	
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Feb-21	4.9	In SystemSettingsValidators, there is a possible permanent denial of service due to missing bounds checks on UI settings. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-156260178 CVE ID : CVE-2021-0338	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/668
Improper Check for Unusual or Exceptional Conditions	10-Feb-21	9.3	In loadAnimation of WindowContainer.java, there is a possible way to keep displaying a malicious app while a target app is brought to the foreground. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-145728687	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/669

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-0339		
Improper Removal of Sensitive Information Before Storage or Transfer	10-Feb-21	9.3	In parseNextBox of IsoInterface.java, there is a possible leak of unredacted location information due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-134155286 CVE ID : CVE-2021-0340	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/670
Improper Certificate Validation	10-Feb-21	5	In verifyHostName of OkHostnameVerifier.java, there is a possible way to accept a certificate for the wrong domain due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-171980069 CVE ID : CVE-2021-0341	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/671
Out-of-bounds Write	04-Feb-21	7.2	In kisd, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not	N/A	O-GOO-ANDR-160221/672

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05449962. CVE ID : CVE-2021-0343		
Not Available	04-Feb-21	7.2	In mtkpower, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05437558. CVE ID : CVE-2021-0344	N/A	O-GOO-ANDR-160221/673
Improper Privilege Management	04-Feb-21	7.2	In mobile_log_d, there is a possible escalation of privilege due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05432974. CVE ID : CVE-2021-0345	N/A	O-GOO-ANDR-160221/674
Out-of-bounds Write	04-Feb-21	7.2	In vpu, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions:	N/A	O-GOO-ANDR-160221/675

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android-11; Patch ID: ALPS05371580. CVE ID : CVE-2021-0346		
Out-of-bounds Read	04-Feb-21	2.1	In ccu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05377188. CVE ID : CVE-2021-0347	N/A	O-GOO-ANDR-160221/676
Out-of-bounds Write	04-Feb-21	7.2	In vpu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05349201. CVE ID : CVE-2021-0348	N/A	O-GOO-ANDR-160221/677
Improper Restriction of Rendered UI Layers or Frames	10-Feb-21	9.3	In PackageInstaller, there is a possible tapjacking attack due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-8.1 Android-9 Android-	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/678

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
			10Android ID: A-155287782 CVE ID : CVE-2021-0302		
Improper Restriction of Rendered UI Layers or Frames	10-Feb-21	9.3	In PackageInstaller, there is a possible tapjacking attack due to an insecure default value. This could lead to local escalation of privilege and permissions with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-154015447 CVE ID : CVE-2021-0305	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/679
Improper Restriction of Rendered UI Layers or Frames	10-Feb-21	6.9	In onCreate of UninstallerActivity, there is a possible way to uninstall an all without informed user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-171221302 CVE ID : CVE-2021-0314	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/680
Out-of-bounds Write	10-Feb-21	9.3	In ih264d_parse_pslice of ih264d_parse_pslice.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/681

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-174238784 CVE ID : CVE-2021-0325		
Out-of-bounds Write	10-Feb-21	10	In p2p_copy_client_info of p2p.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution if the target device is performing a Wi-Fi Direct search, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-172937525 CVE ID : CVE-2021-0326	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/682
Improper Privilege Management	10-Feb-21	7.2	In getContentProviderImpl of ActivityManagerService.java, there is a possible permission bypass due to non-restored binder identities. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/683

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
			172935267 CVE ID : CVE-2021-0327		
Improper Privilege Management	10-Feb-21	7.2	In onBatchScanReports and deliverBatchScan of GattService.java, there is a possible way to retrieve Bluetooth scan results without permissions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-172670415 CVE ID : CVE-2021-0328	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/684
Out-of-bounds Write	10-Feb-21	7.2	In several native functions called by AdvertiseManager.java, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the Bluetooth server with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-171400004 CVE ID : CVE-2021-0329	https://source.android.com/security/bulletin/2021-02-01	O-GOO-ANDR-160221/685
Use After Free	10-Feb-21	7.2	In add_user_ce and remove_user_ce of	https://source.android.com	O-GOO-ANDR-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>stored.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in stored with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-9 Android-10 Android-11 Android ID: A-170732441</p> <p>CVE ID : CVE-2021-0330</p>	m/security/bulletin/2021-02-01	160221/686
Use After Free	04-Feb-21	7.2	<p>In display driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05362646.</p> <p>CVE ID : CVE-2021-0349</p>	N/A	O-GOO-ANDR-160221/687
Improper Input Validation	04-Feb-21	4.9	<p>In ged, there is a possible system crash due to an improper input validation. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05342338.</p> <p>CVE ID : CVE-2021-0350</p>	N/A	O-GOO-ANDR-160221/688
Not Available	04-Feb-21	7.8	<p>In wlan driver, there is a possible system crash due to</p>	N/A	O-GOO-ANDR-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05412917. CVE ID : CVE-2021-0351		160221/689
Access of Resource Using Incompatible Type ('Type Confusion')	03-Feb-21	2.1	In RT regmap driver, there is a possible memory corruption due to type confusion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05453809. CVE ID : CVE-2021-0352	N/A	O-GOO-ANDR-160221/690
Out-of-bounds Write	03-Feb-21	4.6	In kisd, there is a possible memory corruption due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05425247. CVE ID : CVE-2021-0353	N/A	O-GOO-ANDR-160221/691
Out-of-bounds Write	03-Feb-21	4.6	In ged, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System	N/A	O-GOO-ANDR-160221/692

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05431161.</p> <p>CVE ID : CVE-2021-0354</p>		
Integer Overflow or Wraparound	03-Feb-21	4.6	<p>In kisd, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05425581.</p> <p>CVE ID : CVE-2021-0355</p>	N/A	O-GOO-ANDR-160221/693
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-21	4.6	<p>In netdiag, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05442014.</p> <p>CVE ID : CVE-2021-0356</p>	N/A	O-GOO-ANDR-160221/694
Out-of-bounds Write	03-Feb-21	4.6	<p>In netdiag, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.</p>	N/A	O-GOO-ANDR-160221/695

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Product: Android; Versions: Android-11; Patch ID: ALPS05442002. CVE ID : CVE-2021-0357		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-21	4.6	In netdiag, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05442022. CVE ID : CVE-2021-0358	N/A	O-GOO-ANDR-160221/696
Out-of-bounds Write	03-Feb-21	4.6	In netdiag, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05442011. CVE ID : CVE-2021-0359	N/A	O-GOO-ANDR-160221/697
Out-of-bounds Write	03-Feb-21	4.6	In netdiag, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05442006.	N/A	O-GOO-ANDR-160221/698

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-0360		
Out-of-bounds Read	03-Feb-21	4.6	In kisd, there is a possible out of bounds read due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05449968. CVE ID : CVE-2021-0361	N/A	O-GOO-ANDR-160221/699
Out-of-bounds Write	03-Feb-21	4.6	In aee, there is a possible memory corruption due to a stack buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05457070. CVE ID : CVE-2021-0362	N/A	O-GOO-ANDR-160221/700
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Feb-21	4.6	In mobile_log_d, there is a possible command injection due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05458478. CVE ID : CVE-2021-0363	https://corp.mediatek.com/product-security-acknowledgements	O-GOO-ANDR-160221/701
Improper Neutralization	03-Feb-21	4.6	In mobile_log_d, there is a possible command injection	N/A	O-GOO-ANDR-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05458478; Issue ID: ALPS05458503. CVE ID : CVE-2021-0364		160221/702
Use After Free	03-Feb-21	4.6	In display driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android; Versions: Android-11; Patch ID: ALPS05454782. CVE ID : CVE-2021-0365	N/A	O-GOO-ANDR-160221/703
Origin Validation Error	09-Feb-21	4.3	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21136	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html	O-GOO-ANDR-160221/704
Not Available	04-Feb-21	7.5	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. In preloaded applications, the HostnameVerified default is mishandled. The LG ID is	https://lgsecurity.lge.com/	O-GOO-ANDR-160221/705

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			LVE-SMP-200029 (February 2021). CVE ID : CVE-2021-26687		
Not Available	04-Feb-21	7.5	An issue was discovered on LG Wing mobile devices with Android OS 10 software. The biometric sensor has weak security properties. The LG ID is LVE-SMP-200030 (February 2021). CVE ID : CVE-2021-26688	https://lgsecurity.lge.com/	O-GOO-ANDR-160221/706
Use After Free	04-Feb-21	7.5	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. The USB laf gadget has a use-after-free. The LG ID is LVE-SMP-200031 (February 2021). CVE ID : CVE-2021-26689	https://lgsecurity.lge.com/	O-GOO-ANDR-160221/707

hpe

baseboard_management_controller

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webstartflash function. CVE ID : CVE-2021-25142	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/708
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webupdatecomponent function. CVE ID : CVE-2021-25168	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf0408	O-HPE-BASE-160221/709

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetservicecfg function. CVE ID : CVE-2021-25169	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetremoteimageinfo function. CVE ID : CVE-2021-25170	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/711
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetlicensecfg function. CVE ID : CVE-2021-25171	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/712
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so websetdefaultlangcfg function. CVE ID : CVE-2021-25172	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/713
Buffer Copy without	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in	https://support.hpe.com/	O-HPE-BASE-160221/714

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webifc_setadconfig function. CVE ID : CVE-2021-26570	hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg function. CVE ID : CVE-2021-26571	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/715
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg function. CVE ID : CVE-2021-26572	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgeneratesslcfg function. CVE ID : CVE-2021-26573	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/717
Improper Limitation of a Pathname to a Restricted Directory	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletevideofile	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=	O-HPE-BASE-160221/718

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			function. CVE ID : CVE-2021-26574	emr_na-hpesbhf04080en_us	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletesolvideofile function. CVE ID : CVE-2021-26575	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/719
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so uploadsshkey function. CVE ID : CVE-2021-26576	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so uploadsshkey function. CVE ID : CVE-2021-26577	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	O-HPE-BASE-160221/721

Huawei

ecns280_firmware

Uncontrolled Resource Consumption	06-Feb-21	7.8	There is a denial of service (DoS) vulnerability in eCNS280 versions V100R005C00, V100R005C10. Due to a design defect, remote unauthorized attackers send	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210113-	O-HUA-ECNS-160221/722
-----------------------------------	-----------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a large number of specific messages to affected devices, causing system resource exhaustion and web application DoS. CVE ID : CVE-2021-22292	02-dos-en	

smc2.0_firmware

Improper Privilege Management	06-Feb-21	4.6	<p>There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specific commands to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. Affected product versions include: ManageOne versions</p> <p>6.5.0,6.5.0.SPC100.B210,6.5.1.1.B010,6.5.1.1.B020,6.5.1.1.B030,6.5.1.1.B040,6.5.1.SPC100.B050,6.5.1.SPC101.B010,6.5.1.SPC101.B040,6.5.1.SPC200,6.5.1.SPC200.B010,6.5.1.SPC200.B030,6.5.1.SPC200.B040,6.5.1.SPC200.B050,6.5.1.SPC200.B060,6.5.1.SPC200.B070,6.5.1RC1.B060,6.5.1RC2.B020,6.5.1RC2.B030,6.5.1RC2.B040,6.5.1RC2.B050,6.5.1RC2.B060,6.5.1RC2.B070,6.5.1RC2.B080,6.5.1RC2.B090,6.5.RC2.B050,8.0.0,8.0.0-LCND81,8.0.0.SPC100,8.0.1,8.0.RC2,8.0.RC3,8.0.RC3.B041,8.0.RC3.SPC100;</p> <p>NFV_FusionSphere versions 6.5.1.SPC23,8.0.0.SPC12;</p> <p>SMC2.0 versions</p>	<p>https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-02-privilege-en</p>	O-HUA-SMC2-160221/723
-------------------------------	-----------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V600R019C00,V600R019C10 ; iMaster MAE-M versions MAE-TOOL(FusionSphereBasicTemplate_Euler_X86)V100R020C10SPC220. CVE ID : CVE-2021-22299		
ecns280_td_firmware					
Cleartext Storage of Sensitive Information	06-Feb-21	1.9	There is an information leak vulnerability in eCNS280_TD versions V100R005C00 and V100R005C10. A command does not have timeout exit mechanism. Temporary file contains sensitive information. This allows attackers to obtain information by inter-process access that requires other methods. CVE ID : CVE-2021-22300	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-cgp-en	O-HUA-ECNS-160221/724
taurus-al00a_firmware					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Feb-21	5	Some Huawei products have an inconsistent interpretation of HTTP requests vulnerability. Attackers can exploit this vulnerability to cause information leak. Affected product versions include: CampusInsight versions V100R019C10; ManageOne versions 6.5.1.1, 6.5.1.SPC100, 6.5.1.SPC200, 6.5.1RC1, 6.5.1RC2, 8.0.RC2. Affected product versions include: Taurus-AL00A versions 10.0.0.1(C00E1R1P1).	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-01-http-en	O-HUA-TAUR-160221/725

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-22293		
Out-of-bounds Read	06-Feb-21	3.6	There is an out-of-bound read vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module does not verify the some input. Attackers can exploit this vulnerability by sending malicious input through specific app. This could cause out-of-bound, compromising normal service. CVE ID : CVE-2021-22302	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-smartphone-en	O-HUA-TAUR-160221/726
Double Free	06-Feb-21	4.3	There is a pointer double free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). There is a lack of muti-thread protection when a function is called. Attackers can exploit this vulnerability by performing malicious operation to cause pointer double free. This may lead to module crash, compromising normal service. CVE ID : CVE-2021-22303	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-02-smartphone-en	O-HUA-TAUR-160221/727
Use After Free	06-Feb-21	2.1	There is a use after free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module may refer to some memory after it has been freed while dealing with some messages. Attackers can exploit this vulnerability by sending specific message to the affected module. This may lead to module crash, compromising normal service.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-03-smartphone-en	O-HUA-TAUR-160221/728

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-22304		
mate_30_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Feb-21	4.6	Mate 30 10.0.0.203(C00E201R7P2) have a buffer overflow vulnerability. After obtaining the root permission, an attacker can exploit the vulnerability to cause buffer overflow. CVE ID : CVE-2021-22301	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-buffer-en	O-HUA-MATE-160221/729
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Feb-21	2.1	There is a buffer overflow vulnerability in Mate 30 10.1.0.126(C00E125R5P3). A module does not verify the some input when dealing with messages. Attackers can exploit this vulnerability by sending malicious input through specific module. This could cause buffer overflow, compromising normal service. CVE ID : CVE-2021-22305	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-04-smartphone-en	O-HUA-MATE-160221/730
Out-of-bounds Read	06-Feb-21	2.1	There is an out-of-bound read vulnerability in Mate 30 10.0.0.182(C00E180R6P2). A module does not verify the some input when dealing with messages. Attackers can exploit this vulnerability by sending malicious input through specific module. This could cause out-of-bound, compromising normal service. CVE ID : CVE-2021-22306	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-05-smartphone-en	O-HUA-MATE-160221/731
Not Available	06-Feb-21	2.1	There is a weak algorithm	https://www	O-HUA-

CVSS Scoring Scale	0-1	1-2	2-3	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 in Mate 3010.0.0.203(C00E201R7P2). The protection is insufficient for the modules that should be protected. Local attackers can exploit this vulnerability to affect the integrity of certain module. CVE ID : CVE-2021-22307	.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-06-smartphone-en	MATE-160221/732

Linux

linux_kernel

Use of a Broken or Risky Cryptographic Algorithm	12-Feb-21	4	IBM Security Verify Information Queue 1.0.6 and 1.0.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 198184. CVE ID : CVE-2021-20406	https://exchange.xforce.ibmcloud.com/vulnerabilities/196184 , https://www.ibm.com/support/pages/node/6414763	O-LIN-LINU-160221/733
Cleartext Storage of Sensitive Information	12-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 discloses sensitive information in source code that could be used in further attacks against the system. IBM X-Force ID: 198185. CVE ID : CVE-2021-20407	https://exchange.xforce.ibmcloud.com/vulnerabilities/196185 , https://www.ibm.com/support/pages/node/6414765	O-LIN-LINU-160221/734
Cleartext Storage of Sensitive Information	12-Feb-21	2.1	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could disclose highly sensitive information to a local user due to improper storage of a plaintext cryptographic key. IBM X-Force ID: 198187.	https://exchange.xforce.ibmcloud.com/vulnerabilities/196187 , https://www.ibm.com/support/pages/	O-LIN-LINU-160221/735

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-20408	node/6414767	
Exposure of Sensitive Information to an Unauthorized Actor	12-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 198188. CVE ID : CVE-2021-20409	https://exchange.xforce.ibmcloud.com/vulnerabilities/196188 , https://www.ibm.com/support/pages/node/6414771	O-LIN-LINU-160221/736
Cleartext Storage of Sensitive Information	12-Feb-21	3.5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 sends user credentials in plain clear text which can be read by an authenticated user using man in the middle techniques. IBM X-Force ID: 198190. CVE ID : CVE-2021-20410	https://exchange.xforce.ibmcloud.com/vulnerabilities/196190 , https://www.ibm.com/support/pages/node/6414773	O-LIN-LINU-160221/737
Incorrect Resource Transfer Between Spheres	12-Feb-21	4.8	IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user to impersonate another user on the system due to incorrectly updating the session identifier. IBM X-Force ID: 198191. CVE ID : CVE-2021-20411	https://exchange.xforce.ibmcloud.com/vulnerabilities/196191 , https://www.ibm.com/support/pages/node/6414777	O-LIN-LINU-160221/738
Use of Hard-coded Credentials	12-Feb-21	5	IBM Security Verify Information Queue 1.0.6 and 1.0.7 contains hard-coded	https://exchange.xforce.ibmcloud.com	O-LIN-LINU-160221/739

CVSS Scoring Scale	0-1	1-2	2-3	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, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 198192. CVE ID : CVE-2021-20412	/vulnerabilities/196192, https://www.ibm.com/support/pages/node/6414779	
Improper Privilege Management	05-Feb-21	6.9	A local privilege escalation was discovered in the Linux kernel before 5.10.13. Multiple race conditions in the AF_VSOCK implementation are caused by wrong locking in net/vmw_vsock/af_vsock.c. The race conditions were implicitly introduced in the commits that added VSOCK multi-transport support. CVE ID : CVE-2021-26708	http://www.openwall.com/lists/oss-security/2021/02/05/6 , https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.10.13 , https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c518adafa39f37858697ac9309c6cf1805581446	O-LIN-LINU-160221/740
Use After Free	01-Feb-21	2.1	nbd_add_socket in drivers/block/nbd.c in the Linux kernel through 5.10.12 has an ndb_queue_rq use-after-free that could be triggered by local attackers (with access to the nbd device) via an I/O request at a certain point during device setup, aka CID-	http://www.openwall.com/lists/oss-security/2021/02/01/1 , https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.g	O-LIN-LINU-160221/741

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			b98e762e3d71. CVE ID : CVE-2021-3348	it/commit/?id=b98e762e3d71e893b221f871825dc64694cfb258 , https://www.openwall.com/lists/oss-security/2021/01/28/3	

Logitec

lan-w300n\pgrb_firmware

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-21	7.7	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors. CVE ID : CVE-2021-20638	https://www.elecom.co.jp/news/security/20210126-01/	O-LOG-LAN--160221/742
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-21	7.7	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors. CVE ID : CVE-2021-20639	https://www.elecom.co.jp/news/security/20210126-01/	O-LOG-LAN--160221/743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Feb-21	7.7	Buffer overflow vulnerability in LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute an arbitrary OS command via unspecified vectors. CVE ID : CVE-2021-20640	https://www.elecom.co.jp/news/security/20210126-01/	O-LOG-LAN--160221/744

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Microsoft					
windows					
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21035	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/745
Integer Overflow or Wraparound	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Integer Overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21036	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/746
Improper Limitation of	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074	https://helpx.adobe.com/s	O-MIC-WIND-160221/747

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			(and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Path Traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21037	ecurity/prod ucts/acrobat /apsb21-09.html	
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21038	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/748
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use	https://helpx.adobe.com/security/products/acrobat/apsb21-	O-MIC-WIND-160221/749

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21039	09.html	
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21040	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/750
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a use-after-free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/751

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21041		
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally escalate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21042	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/752
Out-of-bounds Write	11-Feb-21	9.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability when parsing a crafted jpeg file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/753

CVSS Scoring Scale	0-1	1-2	2-3	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 open a malicious file. CVE ID : CVE-2021-21044		
Improper Access Control	11-Feb-21	9.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper access control vulnerability. An unauthenticated attacker could leverage this vulnerability to elevate privileges in the context of the current user. CVE ID : CVE-2021-21045	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/754
Access of Memory Location After End of Buffer	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21046	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/755
Unquoted Search Path or Element	02-Feb-21	1.9	Traccar is an open source GPS tracking system. In Traccar before version 4.12 there is an unquoted Windows binary path vulnerability. Only Windows	https://github.com/traccar/traccar/commit/cc69a9907ac9878db3750aa14ff	O-MIC-WIND-160221/756

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions are impacted. Attacker needs write access to the filesystem on the host machine. If Java path includes a space, then attacker can lift their privilege to the same as Traccar service (system). This is fixed in version 4.12. CVE ID : CVE-2021-21292	edb28626455da, https://github.com/traccar/traccar/security/advisories/GHSA-j75r-7qm5-62q5	
Not Available	05-Feb-21	3.6	NVIDIA GeForce Experience, all versions prior to 3.21, contains a vulnerability in GameStream (rxdiag.dll) where an arbitrary file deletion due to improper handling of log files may lead to denial of service. CVE ID : CVE-2021-1072	https://nvidia.custhelp.com/app/answers/detail/a_id/5155	O-MIC-WIND-160221/757
Out-of-bounds Write	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21017	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/758
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions 2020.013.20074 (and earlier),	https://helpx.adobe.com/security/prod	O-MIC-WIND-160221/759

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
			2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21021	ucts/acrobat/apsb21-09.html	
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21028	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/760
Use After Free	11-Feb-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/761

CVSS Scoring Scale	0-1	1-2	2-3	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 to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21033		
Out-of-bounds Read	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability. An unauthenticated attacker could leverage this vulnerability to locally elevate privileges in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21034	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/762
NULL Pointer Dereference	11-Feb-21	4.3	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a null pointer dereference vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to achieve denial of service in the context of the current user.	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/763

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
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21057		
Improper Input Validation	11-Feb-21	4.3	Adobe Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-21060	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/764
Use After Free	11-Feb-21	4.3	Acrobat Pro DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use-after-free vulnerability when parsing a specially crafted PDF file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a	https://helpx.adobe.com/security/products/acrobat/apsb21-09.html	O-MIC-WIND-160221/765

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. CVE ID : CVE-2021-21061		
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the contents of a scan connection exception file. CVE ID : CVE-2021-25230	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	O-MIC-WIND-160221/766
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific hotfix history file. CVE ID : CVE-2021-25231	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/767
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about the SQL database. CVE ID : CVE-2021-25232	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	O-MIC-WIND-160221/768
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro	https://success.trendmicro.com/solution/000284202	O-MIC-WIND-160221/769

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
Information to an Unauthorized Actor			Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific configuration download file. CVE ID : CVE-2021-25233	o.com/solution/000284202, https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about a specific notification configuration file. CVE ID : CVE-2021-25234	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/770
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS) and OfficeScan XG SP1 could allow an unauthenticated user to obtain information about a content inspection configuration file. CVE ID : CVE-2021-25235	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205	O-MIC-WIND-160221/771
Server-Side Request	04-Feb-21	5	A server-side request forgery (SSRF) information	https://success.trendmicro.com/solution/000284205	O-MIC-WIND-160221/772

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a specific sweep. CVE ID : CVE-2021-25236	o.com/solution/000284205, https://success.trendmicro.com/solution/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem) could allow an unauthenticated user to obtain information about the managing port used by agents. CVE ID : CVE-2021-25237	https://success.trendmicro.com/solution/000284202	O-MIC-WIND-160221/773
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control information disclosure vulnerability in Trend Micro OfficeScan XG SP1 and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about an agent's managing port. CVE ID : CVE-2021-25238	https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/774
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain information about x86 agent hotfixes. CVE ID : CVE-2021-25239	https://success.trendmicro.com/solution/000284202 , https://success.trendmicro.com/solution/000284205 , https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/775

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				on/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain x64 agent hofitx information. CVE ID : CVE-2021-25240	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/776
Server-Side Request Forgery (SSRF)	04-Feb-21	5	A server-side request forgery (SSRF) information disclosure vulnerability in Trend Micro Apex One and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to locate online agents via a sweep. CVE ID : CVE-2021-25241	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/777
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain version and build information. CVE ID : CVE-2021-25242	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/soluti	O-MIC-WIND-160221/778

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				on/000284206	
Exposure of Sensitive Information to an Unauthorized Actor	04-Feb-21	5	An improper access control vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security 10.0 SP1 could allow an unauthenticated user to obtain patch level information. CVE ID : CVE-2021-25243	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/779
Out-of-bounds Read	04-Feb-21	2.1	An out-of-bounds read information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could allow an attacker to disclose sensitive information about a named pipe. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25248	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284205, https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/780
Out-of-bounds Write	04-Feb-21	7.2	An out-of-bounds write information disclosure vulnerability in Trend Micro Apex One (on-prem and SaaS), OfficeScan XG SP1, and Worry-Free Business Security (10.0 SP1 and Services) could	https://success.trendmicro.com/solution/000284202, https://success.trendmicro.com/solution/000284206	O-MIC-WIND-160221/781

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. CVE ID : CVE-2021-25249	o.com/solution/000284205, https://success.trendmicro.com/solution/000284206	

Siemens

scalance_w780_firmware

Allocation of Resources Without Limits or Throttling	09-Feb-21	3.3	A vulnerability has been identified in SCALANCE W780 and W740 (IEEE 802.11n) family (All versions < V6.3). Sending specially crafted packets through the ARP protocol to an affected device could cause a partial denial-of-service, preventing the device to operate normally for a short period of time. CVE ID : CVE-2021-25666	https://certportal.siemens.com/productcert/pdf/sa-686152.pdf	O-SIE-SCAL-160221/782
--	-----------	-----	--	---	-----------------------

scalance_w740_firmware

Allocation of Resources Without Limits or Throttling	09-Feb-21	3.3	A vulnerability has been identified in SCALANCE W780 and W740 (IEEE 802.11n) family (All versions < V6.3). Sending specially crafted packets through the ARP protocol to an affected device could cause a partial denial-of-service, preventing the device to operate normally for a short period of time. CVE ID : CVE-2021-25666	https://certportal.siemens.com/productcert/pdf/sa-686152.pdf	O-SIE-SCAL-160221/783
--	-----------	-----	--	---	-----------------------

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
Sonicwall					
sma_200_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	O-SON-SMA-160221/784
sma_210_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	O-SON-SMA-160221/785
sma_400_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	O-SON-SMA-160221/786

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sma_410_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	O-SON-SMA_-160221/787
sma_100_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	O-SON-SMA_-160221/788
Hardware					
Asus					
rt-ax3000					
Not Available	05-Feb-21	7.8	Denial of service in ASUSWRT ASUS RT-AX3000 firmware versions 3.0.0.4.384_10177 and earlier versions allows an attacker to disrupt the use of device setup services via continuous login error. CVE ID : CVE-2021-3229	https://dlcdnimgs.asus.com/websites/global/productcustomizedTab/562/ASUSWRT%20portal%20feature.pdf , https://www.asus.com/us	H-ASU-RT-A-160221/789

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
				/ASUSWRT/	
Belkin					
linksys_wrt160nl					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Feb-21	9	** UNSUPPORTED WHEN ASSIGNED ** The administration web interface on Belkin Linksys WRT160NL 1.0.04.002_US_20130619 devices allows remote authenticated attackers to execute system commands with root privileges via shell metacharacters in the ui_language POST parameter to the apply.cgi form endpoint. This occurs in do_upgrade_post in mini_httpd. NOTE: This vulnerability only affects products that are no longer supported by the maintainer CVE ID : CVE-2021-25310	N/A	H-BEL-LINK-160221/790
Cisco					
nexus_3600					
Improper Access Control	04-Feb-21	6.4	A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j	H-CIS-NEXU-160221/791

CVSS Scoring Scale	0-1	1-2	2-3	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 crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL. CVE ID : CVE-2021-1389		

rv320_dual_gigabit_wan_vpn_router

Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/792
-----------------------------	-----------	---	---	---	-----------------------

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
			the affected device. CVE ID : CVE-2021-1334		
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1335	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/793
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV32-160221/794

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>	sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/795

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/796

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1338</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/797

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1339		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1340	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/798
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV32-160221/799

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
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1341</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/800

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1342</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/801

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1343</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/802

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
			the affected device. CVE ID : CVE-2021-1344		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1345	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/803
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV32-160221/804

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1346</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/805

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1347</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/806

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1348</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1314</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV32-160221/807

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV32-160221/808
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV32-160221/809

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1316</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV32-160221/810

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1317		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV32-160221/811
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV32-160221/812

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
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/813

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/814

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1321</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/815

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1322		
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1323	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/816
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV32-160221/817

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/818

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/819

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1326</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/820

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
			would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1327		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1328	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/821
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV32-160221/822

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/823

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/824

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1331</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/825

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1332		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1333	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/826
nexus_9500_r					
Improper Access	04-Feb-21	6.4	A vulnerability in the IPv6 traffic processing of Cisco IOS	https://tools.cisco.com/se	H-CIS-NEXU-160221/827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			<p>XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.</p> <p>CVE ID : CVE-2021-1389</p>	<p>curity/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j</p>	

rv160w_wireless-ac_vpn_router

External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV16-160221/828
---	-----------	----	--	--	-----------------------

CVSS Scoring Scale	0-1	1-2	2-3	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 of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289		
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1290	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV16-160221/829
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV16-160221/830

CVSS Scoring Scale	0-1	1-2	2-3	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 HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1291		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1292	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV16-160221/831
External Control of Assumed-Immutable Web	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV16-160221/832

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Parameter			<p>RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1293</p>	visory/cisco-sa-rv160-260-rce-XZeFkNHf	
Not Available	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV16-160221/833

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
			CVE ID : CVE-2021-1294		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1295</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV16-160221/834
Absolute Path Traversal	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn</p>	H-CIS-RV16-160221/835

CVSS Scoring Scale	0-1	1-2	2-3	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 web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1296		
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	H-CIS-RV16-160221/836
rv260_vpn_router					
External Control of Assumed-Immutable	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W,	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV26-160221/837

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Parameter			RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289	coSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/838

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code on the device. CVE ID : CVE-2021-1290		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1291	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/839
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/840

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
			crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1292		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1293	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/841
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-	H-CIS-RV26-160221/842

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1294</p>	XZeFkNHf	
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1295</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/843
Absolute Path	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small</p>	https://tools.cisco.com/security/center	H-CIS-RV26-160221/844

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal			<p>Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device.</p> <p>CVE ID : CVE-2021-1296</p>	/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	
Absolute Path Traversal	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn</p>	H-CIS-RV26-160221/845

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297		
rv260p_vpn_router_with_poe					
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/846
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-	H-CIS-RV26-160221/847

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
			<p>arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1290</p>	XZeFkNHf	
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1291</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV26-160221/848
External Control of	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management</p>	<p>https://tools.cisco.com/se</p>	H-CIS-RV26-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assumed-Immutable Web Parameter			<p>interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1292</p>	<p>curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	160221/849
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV26-160221/850

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1293		
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1294	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/851
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/852

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1295</p>		
Absolute Path Traversal	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device.</p> <p>CVE ID : CVE-2021-1296</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn</p>	H-CIS-RV26-160221/853
Absolute Path Traversal	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn</p>	H-CIS-RV26-160221/854

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297	visory/cisco-sa-rv160-260-filewrite-7x9mnKjn	

rv260w_wireless-ac_vpn_router

External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/855
---	-----------	----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1289		
Not Available	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1290	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/856
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/857

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
			attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1291		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1292	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/858
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-	H-CIS-RV26-160221/859

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1293</p>	260-rce-XZeFkNHf	
Not Available	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1294</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV26-160221/860

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1295	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV26-160221/861
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	H-CIS-RV26-160221/862

CVSS Scoring Scale	0-1	1-2	2-3	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 to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1296		
Absolute Path Traversal	04-Feb-21	9.4	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	H-CIS-RV26-160221/863
rv160_vpn_router					
External Control of Assumed-Immutable Web	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	H-CIS-RV16-160221/864

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Parameter			<p>RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1289</p>	visory/cisco-sa-rv160-260-rce-XZeFkNHf	
Not Available	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV16-160221/865

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1290		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device. CVE ID : CVE-2021-1291	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV16-160221/866
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV16-160221/867

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1292</p>		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1293</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV16-160221/868
Not Available	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf</p>	H-CIS-RV16-160221/869

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1294</p>		
External Control of Assumed-Immutable Web Parameter	04-Feb-21	10	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code as the root user on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.</p> <p>CVE ID : CVE-2021-1295</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-rce-XZeFkNHf	H-CIS-RV16-160221/870
Absolute Path Traversal	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W,</p>	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV16-160221/871

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device.</p> <p>CVE ID : CVE-2021-1296</p>	coSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn	
Absolute Path Traversal	04-Feb-21	9.4	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn</p>	H-CIS-RV16-160221/872

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that they should not have access to. A successful exploit could allow the attacker to overwrite files on the file system of the affected device. CVE ID : CVE-2021-1297		
rv016_multi-wan_vpn_router					
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1334	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/873

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/874
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV01-160221/875

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1336	ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/876

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/877

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1338</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/878

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
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/879
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	H-CIS-RV01-160221/880

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1341	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/881

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1342</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/882

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1343</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/883

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/884
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV01-160221/885

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
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1346	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/886

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1347</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/887

CVSS Scoring Scale	0-1	1-2	2-3	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 to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1314	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV01-160221/888
Improper Neutralization of Special	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	H-CIS-RV01-160221/889

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315	/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV01-160221/890

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1316</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV01-160221/891

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
			valid administrator credentials on an affected device. CVE ID : CVE-2021-1317		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV01-160221/892
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV01-160221/893

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/894

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/895

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
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/896

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1322		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/897
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV01-160221/898

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/899

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/900

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/901

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
			CVE ID : CVE-2021-1327		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/902
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV01-160221/903

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/904

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV01-160221/905

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/906

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1332		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1333	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV01-160221/907
rv042_dual_wan_vpn_router					
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV04-160221/908

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1334</p>	sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/909

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/910

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/911

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
			the affected device. CVE ID : CVE-2021-1337		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1338	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/912
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV04-160221/913

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/914

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
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/915

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1341</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/916

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1342		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1343	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/917
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV04-160221/918

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/919

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/920

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1346</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/921

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1347		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/922
Improper Neutralization of Special Elements used in a Command	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV04-160221/923

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			<p>an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1314</p>	sa-rv-command-inject-BY4c5zd	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV04-160221/924

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV04-160221/925

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1316		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1317</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV04-160221/926
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV04-160221/927

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
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1318</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/929

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1320		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/930
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/931

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1322</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/932

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/933

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/934

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1325		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/935
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/936

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1327</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/937

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
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/938

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/939

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1330		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/940
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/941

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1332</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/942

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1333</p>		

rv042g_dual_gigabit_wan_vpn_router

Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/943
-----------------------------	-----------	---	--	--	-----------------------

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
			could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1334		
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/944

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1335		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1336	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/945
Out-of-bounds Write	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV04-160221/946

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/947

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1338</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/948

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/949

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1340		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1341	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/950
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV04-160221/951

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1342</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/952

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1343</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/953

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/954

CVSS Scoring Scale	0-1	1-2	2-3	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 need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1345		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1346	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/955
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://tools.cisco.com/security/center/content/Cis	H-CIS-RV04-160221/956

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1347</p>	coSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/957

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1348</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV04-160221/958

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1314		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV04-160221/959
Improper Neutralization	04-Feb-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	H-CIS-RV04-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1316	curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	160221/960
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV04-160221/961

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1317</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV04-160221/962

CVSS Scoring Scale	0-1	1-2	2-3	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 would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1319	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/963
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	H-CIS-RV04-160221/964

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow			<p>Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/965

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1321</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/966

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1322</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/967

CVSS Scoring Scale	0-1	1-2	2-3	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, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1323		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1324	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/968
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	H-CIS-RV04-160221/969

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
Overflow			<p>Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/970

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1326</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/971

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1327</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/972

CVSS Scoring Scale	0-1	1-2	2-3	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, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1328		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1329	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/973
Stack-based Buffer	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	H-CIS-RV04-160221/974

CVSS Scoring Scale	0-1	1-2	2-3	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			<p>Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>	/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV04-160221/975

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
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1331</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/976

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1332</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV04-160221/977

CVSS Scoring Scale	0-1	1-2	2-3	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, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1333		
rv082_dual_wan_vpn_router					
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1334	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/978
Out-of-	04-Feb-21	9	Multiple vulnerabilities in the	https://tools.	H-CIS-RV08-

CVSS Scoring Scale	0-1	1-2	2-3	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 Write			<p>web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	160221/979
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/980

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
			<p>device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/981

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1337</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/982

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1338</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/983

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/984
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-	H-CIS-RV08-160221/985

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1341	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/986

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1342</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/987

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1343</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/988

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
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/989
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-</p>	H-CIS-RV08-160221/990

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1346	ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/991

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1347</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/992

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
			device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1314	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV08-160221/993
Improper Neutralization of Special	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	H-CIS-RV08-160221/994

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315	/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV08-160221/995

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
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1316</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV08-160221/996

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			valid administrator credentials on an affected device. CVE ID : CVE-2021-1317		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1318	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV08-160221/997
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV08-160221/998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/999

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
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1320</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/1000

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/1001

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1322		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/1002
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV08-160221/1003

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/1004

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1325</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/1005

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/1006

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1327		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/1007
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV08-160221/1008

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>	overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface.</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/1009

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
			<p>An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1330</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV08-160221/1010

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/1011

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1332		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1333	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV08-160221/1012
rv325_dual_gigabit_wan_vpn_router					
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV32-160221/1013

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1334</p>	sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1014

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1335</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1015

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1336</p>		
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1016

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1337		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1338	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1017
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV32-160221/1018

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1339</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1019

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1340</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1020

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1341</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1021

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1342		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1343	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1022
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV32-160221/1023

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1344</p>	sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1024

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1345</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1025

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1346</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1026

CVSS Scoring Scale	0-1	1-2	2-3	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 affected device. CVE ID : CVE-2021-1347		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1348	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1027
Improper Neutralization of Special Elements used in a Command	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-RV32-160221/1028

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			<p>an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1314</p>	sa-rv-command-inject-BY4c5zd	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd</p>	H-CIS-RV32-160221/1029

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
			requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device. CVE ID : CVE-2021-1315		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV32-160221/1030

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-1316		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1317</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV32-160221/1031
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. These</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-command-inject-BY4c5zd	H-CIS-RV32-160221/1032

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on an affected device.</p> <p>CVE ID : CVE-2021-1318</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1033

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1319</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1034

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1320		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1321	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1035
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1036

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1322</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Out-of-bounds Write	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1037

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1323</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1038

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1324</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1039

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1325		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1326	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1040
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1041

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1327</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1042

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1328</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1043

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1329</p>		
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1044

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator credentials on the affected device. CVE ID : CVE-2021-1330		
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. CVE ID : CVE-2021-1331	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1045
Stack-based Buffer Overflow	04-Feb-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj	H-CIS-RV32-160221/1046

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1332</p>	visory/cisco-sa-rv-overflow-ghZP68yj	
Stack-based Buffer Overflow	04-Feb-21	9	<p>Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly. These vulnerabilities are due to improper validation of user-</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-ghZP68yj</p>	H-CIS-RV32-160221/1047

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>supplied input in the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.</p> <p>CVE ID : CVE-2021-1333</p>		

8201

Improper Verification of Cryptographic Signature	04-Feb-21	4.6	<p>Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.</p> <p>CVE ID : CVE-2021-1244</p>	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	H-CIS-8201-160221/1048
Improper Verification of	04-Feb-21	4.6	<p>Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series</p>	https://tools.cisco.com/security/center	H-CIS-8201-160221/1049

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Signature			Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1136	/content/CiscoSecurityAdvisory/cisco-sa-ioxr-lzNhcGCBt	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-21	7.2	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running NCS540L software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device. The vulnerability is due to insufficient validation of command line arguments. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level privileges to escalate their privilege level to root. CVE ID : CVE-2021-1370	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pe-QpzCAePe	H-CIS-8201-160221/1050

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
8202					
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1244	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-lzNhcGCBt	H-CIS-8202-160221/1051
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1136	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-lzNhcGCBt	H-CIS-8202-160221/1052
Improper Neutralization of Special Elements used in an OS Command	04-Feb-21	7.2	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-8202-160221/1053

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			NCS540L software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device. The vulnerability is due to insufficient validation of command line arguments. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level privileges to escalate their privilege level to root. CVE ID : CVE-2021-1370	sa-iosxr-pe-QpzCAePe	

8808

Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1244	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	H-CIS-8808-160221/1054
Improper Verification	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence	https://tools.cisco.com/se	H-CIS-8808-160221/1055

CVSS Scoring Scale	0-1	1-2	2-3	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 Cryptographic Signature			System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1136	curity/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-21	7.2	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running NCS540L software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device. The vulnerability is due to insufficient validation of command line arguments. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level privileges to escalate their privilege level to root. CVE ID : CVE-2021-1370	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pe-QpzCAePe	H-CIS-8808-160221/1056

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
8812					
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1244	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	H-CIS-8812-160221/1057
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1136	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	H-CIS-8812-160221/1058
Improper Neutralization of Special Elements used in an OS Command	04-Feb-21	7.2	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-8812-160221/1059

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			NCS540L software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device. The vulnerability is due to insufficient validation of command line arguments. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level privileges to escalate their privilege level to root. CVE ID : CVE-2021-1370	sa-iosxr-pe-QpzCAePe	

8818

Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1244	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	H-CIS-8818-160221/1060
Improper Verification	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence	https://tools.cisco.com/se	H-CIS-8818-160221/1061

CVSS Scoring Scale	0-1	1-2	2-3	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 Cryptographic Signature			System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1136	curity/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-21	7.2	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running NCS540L software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device. The vulnerability is due to insufficient validation of command line arguments. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level privileges to escalate their privilege level to root. CVE ID : CVE-2021-1370	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pe-QpzCAePe	H-CIS-8818-160221/1062

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ncs_1001					
Insufficient Adherence to Expected Conventions	04-Feb-21	3.3	<p>A vulnerability in the IPv6 protocol handling of the management interfaces of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause an IPv6 flood on the management interface network of an affected device. The vulnerability exists because the software incorrectly forwards IPv6 packets that have an IPv6 node-local multicast group address destination and are received on the management interfaces. An attacker could exploit this vulnerability by connecting to the same network as the management interfaces and injecting IPv6 packets that have an IPv6 node-local multicast group address destination. A successful exploit could allow the attacker to cause an IPv6 flood on the corresponding network. Depending on the number of Cisco IOS XR Software nodes on that network segment, exploitation could cause excessive network traffic, resulting in network degradation or a denial of service (DoS) condition.</p> <p>CVE ID : CVE-2021-1268</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K</p>	H-CIS-NCS_-160221/1063
ncs_1002					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Adherence to Expected Conventions	04-Feb-21	3.3	<p>A vulnerability in the IPv6 protocol handling of the management interfaces of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause an IPv6 flood on the management interface network of an affected device. The vulnerability exists because the software incorrectly forwards IPv6 packets that have an IPv6 node-local multicast group address destination and are received on the management interfaces. An attacker could exploit this vulnerability by connecting to the same network as the management interfaces and injecting IPv6 packets that have an IPv6 node-local multicast group address destination. A successful exploit could allow the attacker to cause an IPv6 flood on the corresponding network. Depending on the number of Cisco IOS XR Software nodes on that network segment, exploitation could cause excessive network traffic, resulting in network degradation or a denial of service (DoS) condition.</p> <p>CVE ID : CVE-2021-1268</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K</p>	H-CIS-NCS_-160221/1064
ncs_5501					
Improper Access	04-Feb-21	6.4	<p>A vulnerability in the IPv6 traffic processing of Cisco IOS</p>	<p>https://tools.cisco.com/se</p>	H-CIS-NCS_-160221/1065

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			<p>XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.</p> <p>CVE ID : CVE-2021-1389</p>	<p>curity/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j</p>	

ncs_5501-se

Improper Access Control	04-Feb-21	6.4	<p>A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j</p>	H-CIS-NCS_-160221/1066
-------------------------	-----------	-----	---	--	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL. CVE ID : CVE-2021-1389		

ncs_5502

Improper Access Control	04-Feb-21	6.4	A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL. CVE ID : CVE-2021-1389	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j	H-CIS-NCS_-160221/1067
-------------------------	-----------	-----	---	---	------------------------

ncs_5502-se

Improper Access Control	04-Feb-21	6.4	A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-NCS_-160221/1068
-------------------------	-----------	-----	---	---	------------------------

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
			<p>attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.</p> <p>CVE ID : CVE-2021-1389</p>	sa-ipv6-acl-CHgdYk8j	

ncs_5508

Improper Access Control	04-Feb-21	6.4	<p>A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j</p>	H-CIS-NCS_-160221/1069
-------------------------	-----------	-----	--	--	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			typically be protected by the interface ACL. CVE ID : CVE-2021-1389		
ncs_5516					
Improper Access Control	04-Feb-21	6.4	A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL. CVE ID : CVE-2021-1389	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j	H-CIS-NCS_-160221/1070
ncs_540					
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	H-CIS-NCS_-160221/1071

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1244		
Improper Verification of Cryptographic Signature	04-Feb-21	4.6	Multiple vulnerabilities in Cisco Network Convergence System (NCS) 540 Series Routers, only when running Cisco IOS XR NCS540L software images, and Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. CVE ID : CVE-2021-1136	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt	H-CIS-NCS_-160221/1072
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Feb-21	7.2	A vulnerability in a CLI command of Cisco IOS XR Software for the Cisco 8000 Series Routers and Network Convergence System 540 Series Routers running NCS540L software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device. The vulnerability is due to insufficient validation of command line arguments. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pe-QpzCAePe	H-CIS-NCS_-160221/1073

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticating to the device and entering a crafted command at the prompt. A successful exploit could allow an attacker with low-level privileges to escalate their privilege level to root.</p> <p>CVE ID : CVE-2021-1370</p>		
Improper Access Control	04-Feb-21	6.4	<p>A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.</p> <p>CVE ID : CVE-2021-1389</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j</p>	H-CIS-NCS_-160221/1074
ncs_560					
Improper Access Control	04-Feb-21	6.4	<p>A vulnerability in the IPv6 traffic processing of Cisco IOS XR Software and Cisco NX-OS Software for certain Cisco devices could allow an unauthenticated, remote</p>	<p>https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-</p>	H-CIS-NCS_-160221/1075

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to bypass an IPv6 access control list (ACL) that is configured for an interface of an affected device. The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. A successful exploit could allow the attacker to access resources that would typically be protected by the interface ACL.</p> <p>CVE ID : CVE-2021-1389</p>	sa-ipv6-acl-CHgdYk8j	

elecom

wrc-300feb-k-a

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Feb-21	4.3	<p>Cross-site scripting vulnerability in ELECOM WRC-300FEBK-A allows remote authenticated attackers to inject arbitrary script via unspecified vectors.</p> <p>CVE ID : CVE-2021-20645</p>	https://www.elecom.co.jp/news/security/20210126-01/	H-ELE-WRC--160221/1076
--	-----------	-----	---	---	------------------------

Cross-Site Request Forgery (CSRF)	12-Feb-21	4.3	<p>Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-A allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started.</p>	https://www.elecom.co.jp/news/security/20210126-01/	H-ELE-WRC--160221/1077
-----------------------------------	-----------	-----	---	---	------------------------

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-20646		
wrc-300febks					
Cross-Site Request Forgery (CSRF)	12-Feb-21	4.3	Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-S allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started. CVE ID : CVE-2021-20647	https://www.elecom.co.jp/news/security/20210126-01/	H-ELE-WRC--160221/1078
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-21	7.7	ELECOM WRC-300FEBK-S allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors. CVE ID : CVE-2021-20648	https://www.elecom.co.jp/news/security/20210126-01/	H-ELE-WRC--160221/1079
Improper Certificate Validation	12-Feb-21	5.8	ELECOM WRC-300FEBK-S contains an improper certificate validation vulnerability. Via a man-in-the-middle attack, an attacker may alter the communication response. As a result, an arbitrary OS command may be executed on the affected device. CVE ID : CVE-2021-20649	https://www.elecom.co.jp/news/security/20210126-01/	H-ELE-WRC--160221/1080
fiberhome					
hg6245d					
Not Available	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices	N/A	H-FIB-HG62-160221/1081

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through RP2613. It is possible to extract information from the device without authentication by disabling JavaScript and visiting /info.asp. CVE ID : CVE-2021-27139		
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to find passwords and authentication cookies stored in cleartext in the web.log HTTP logs. CVE ID : CVE-2021-27140	N/A	H-FIB-HG62-160221/1082
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. Credentials in /fhconf/umconfig.txt are obfuscated via XOR with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*^#@s0i3g key. (The webs binary has details on how XOR is used.) CVE ID : CVE-2021-27141	N/A	H-FIB-HG62-160221/1083
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web management is done over HTTPS, using a hardcoded private key that has 0777 permissions. CVE ID : CVE-2021-27142	N/A	H-FIB-HG62-160221/1084
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the	N/A	H-FIB-HG62-160221/1085

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
			hardcoded user / user1234 credentials for an ISP. CVE ID : CVE-2021-27143		
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded f~!b@e#r\$h%o^m*esuperadmin / s(f)u_h+g u credentials for an ISP. CVE ID : CVE-2021-27144	N/A	H-FIB-HG62-160221/1086
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / lnadmin credentials for an ISP. CVE ID : CVE-2021-27145	N/A	H-FIB-HG62-160221/1087
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / CUadmin credentials for an ISP. CVE ID : CVE-2021-27146	N/A	H-FIB-HG62-160221/1088
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / admin credentials for an ISP. CVE ID : CVE-2021-27147	N/A	H-FIB-HG62-160221/1089
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded telecomadmin /	N/A	H-FIB-HG62-160221/1090

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			nE7jA%5m credentials for an ISP. CVE ID : CVE-2021-27148		
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded adminpldt / z6dUABtl270qRxt7a2uGTiw credentials for an ISP. CVE ID : CVE-2021-27149	N/A	H-FIB-HG62-160221/1091
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded gestiontelebucaramanga / t3l3buc4r4m4ng42013 credentials for an ISP. CVE ID : CVE-2021-27150	N/A	H-FIB-HG62-160221/1092
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded rootmet / m3tr0r00t credentials for an ISP. CVE ID : CVE-2021-27151	N/A	H-FIB-HG62-160221/1093
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded awnfibre / fibre@dm!n credentials for an ISP. CVE ID : CVE-2021-27152	N/A	H-FIB-HG62-160221/1094
Use of Hard-coded	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices	N/A	H-FIB-HG62-160221/1095

CVSS Scoring Scale	0-1	1-2	2-3	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			through RP2613. The web daemon contains the hardcoded trueadmin / admintrue credentials for an ISP. CVE ID : CVE-2021-27153		
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / G0R2U1P2ag credentials for an ISP. CVE ID : CVE-2021-27154	N/A	H-FIB-HG62-160221/1096
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 3UJUh2VemEfUtesEchEC2d2e credentials for an ISP. CVE ID : CVE-2021-27155	N/A	H-FIB-HG62-160221/1097
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains credentials for an ISP that equal the last part of the MAC address of the br0 interface. CVE ID : CVE-2021-27156	N/A	H-FIB-HG62-160221/1098
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 888888 credentials for an ISP. CVE ID : CVE-2021-27157	N/A	H-FIB-HG62-160221/1099
Use of Hard-	10-Feb-21	7.5	An issue was discovered on	N/A	H-FIB-HG62-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
coded Credentials			FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded L1vt1m4eng / 888888 credentials for an ISP. CVE ID : CVE-2021-27158		160221/1100						
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded useradmin / 888888 credentials for an ISP. CVE ID : CVE-2021-27159	N/A	H-FIB-HG62-160221/1101						
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / 888888 credentials for an ISP. CVE ID : CVE-2021-27160	N/A	H-FIB-HG62-160221/1102						
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / 1234 credentials for an ISP. CVE ID : CVE-2021-27161	N/A	H-FIB-HG62-160221/1103						
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded user / tattoo@home credentials for an ISP. CVE ID : CVE-2021-27162	N/A	H-FIB-HG62-160221/1104						
Use of Hard-	10-Feb-21	7.5	An issue was discovered on	N/A	H-FIB-HG62-						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
coded Credentials			FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / tele1234 credentials for an ISP. CVE ID : CVE-2021-27163		160221/1105					
Use of Hard-coded Credentials	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. The web daemon contains the hardcoded admin / aisadmin credentials for an ISP. CVE ID : CVE-2021-27164	N/A	H-FIB-HG62-160221/1106					
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The telnet daemon on port 23/tcp can be abused with the gpon/gpon credentials. CVE ID : CVE-2021-27165	N/A	H-FIB-HG62-160221/1107					
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. The password for the enable command is gpon. CVE ID : CVE-2021-27166	N/A	H-FIB-HG62-160221/1108					
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a password of four hexadecimal characters for the admin account. These characters are generated in init_3bb_password in libci_adaptation_layer.so. CVE ID : CVE-2021-27167	N/A	H-FIB-HG62-160221/1109					
Use of Hard-coded	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices	N/A	H-FIB-HG62-160221/1110					
CVSS Scoring Scale	0-1	1-2	2-3	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			through RP2613. There is a 6GFjdY4aAuUKjdtSn7d password for the rdsadmin account. CVE ID : CVE-2021-27168		
Insecure Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. By default, there are no firewall rules for IPv6 connectivity, exposing the internal management interfaces to the Internet. CVE ID : CVE-2021-27170	N/A	H-FIB-HG62-160221/1111
Out-of-bounds Write	10-Feb-21	10	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to start a Linux telnetd as root on port 26/tcp by using the CLI interface commands of ddd and shell (or tshell). CVE ID : CVE-2021-27171	N/A	H-FIB-HG62-160221/1112
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. A hardcoded GEAPON password for root is defined inside /etc/init.d/system-config.sh. CVE ID : CVE-2021-27172	N/A	H-FIB-HG62-160221/1113
Improper Authentication	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. There is a telnet?enable=0&key=calculated(BR0_MAC) backdoor API, without authentication, provided by the HTTP server. This will remove firewall rules and allow an attacker to	N/A	H-FIB-HG62-160221/1114

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
			reach the telnet server (used for the CLI). CVE ID : CVE-2021-27173		
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. wifi_custom.cfg has cleartext passwords and 0644 permissions. CVE ID : CVE-2021-27174	N/A	H-FIB-HG62-160221/1115
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_2g.cfg has cleartext passwords and 0644 permissions. CVE ID : CVE-2021-27175	N/A	H-FIB-HG62-160221/1116
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. wifictl_5g.cfg has cleartext passwords and 0644 permissions. CVE ID : CVE-2021-27176	N/A	H-FIB-HG62-160221/1117
Incorrect Authorization	10-Feb-21	7.5	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to bypass authentication by sending the decoded value of the GgpoZWxwCmxc3QKd2hvcg== string to the telnet server. CVE ID : CVE-2021-27177	N/A	H-FIB-HG62-160221/1118
Cleartext Storage of Sensitive Information	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. Some passwords are stored in	N/A	H-FIB-HG62-160221/1119

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cleartext in nvram. CVE ID : CVE-2021-27178		
Improper Input Validation	10-Feb-21	5	An issue was discovered on FiberHome HG6245D devices through RP2613. It is possible to crash the telnet daemon by sending a certain 0a 65 6e 61 62 6c 65 0a 02 0a 1a 0a string. CVE ID : CVE-2021-27179	N/A	H-FIB-HG62-160221/1120
an5506-04-fa					
Use of Hard-coded Credentials	10-Feb-21	5	An issue was discovered on FiberHome AN5506-04-FA devices with firmware RP2631. There is a gepon password for the gepon account. CVE ID : CVE-2021-27169	N/A	H-FIB-AN55-160221/1121
hpe					
apollo_70_system					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webstartflash function. CVE ID : CVE-2021-25142	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1122
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webupdatecomponent function. CVE ID : CVE-2021-25168	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf0408	H-HPE-APOL-160221/1123

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetservicecfg function. CVE ID : CVE-2021-25169	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1124
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetremoteimageinfo function. CVE ID : CVE-2021-25170	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1125
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so websetlicensecfg function. CVE ID : CVE-2021-25171	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1126
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so websetdefaultlangcfg function. CVE ID : CVE-2021-25172	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1127
Buffer Copy without	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in	https://support.hpe.com/	H-HPE-APOL-160221/1128

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webifc_setadconfig function. CVE ID : CVE-2021-26570	hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg function. CVE ID : CVE-2021-26571	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1129
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgetactivexcfg function. CVE ID : CVE-2021-26572	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1130
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so webgeneratesslcfg function. CVE ID : CVE-2021-26573	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1131
Improper Limitation of a Pathname to a Restricted Directory	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletevideofile	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=	H-HPE-APOL-160221/1132

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			function. CVE ID : CVE-2021-26574	emr_na-hpesbhf04080en_us	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a path traversal vulnerability in libifc.so webdeletesolvideofile function. CVE ID : CVE-2021-26575	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1133
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a command injection vulnerability in libifc.so uploadsshkey function. CVE ID : CVE-2021-26576	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1134
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Feb-21	7.2	The Baseboard Management Controller (BMC) firmware in HPE Apollo 70 System prior to version 3.0.14.0 has a local buffer overflow in libifc.so uploadsshkey function. CVE ID : CVE-2021-26577	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04080en_us	H-HPE-APOL-160221/1135
Huawei					
ecns280					
Uncontrolled Resource Consumption	06-Feb-21	7.8	There is a denial of service (DoS) vulnerability in eCNS280 versions V100R005C00, V100R005C10. Due to a design defect, remote unauthorized attackers send	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210113-	H-HUA-ECNS-160221/1136

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a large number of specific messages to affected devices, causing system resource exhaustion and web application DoS. CVE ID : CVE-2021-22292	02-dos-en	

smc2.0

Improper Privilege Management	06-Feb-21	4.6	<p>There is a local privilege escalation vulnerability in some Huawei products. A local, authenticated attacker could craft specific commands to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. Affected product versions include: ManageOne versions</p> <p>6.5.0,6.5.0.SPC100.B210,6.5.1.1.B010,6.5.1.1.B020,6.5.1.1.B030,6.5.1.1.B040,6.5.1.SPC100.B050,6.5.1.SPC101.B010,6.5.1.SPC101.B040,6.5.1.SPC200,6.5.1.SPC200.B010,6.5.1.SPC200.B030,6.5.1.SPC200.B040,6.5.1.SPC200.B050,6.5.1.SPC200.B060,6.5.1.SPC200.B070,6.5.1RC1.B060,6.5.1RC2.B020,6.5.1RC2.B030,6.5.1RC2.B040,6.5.1RC2.B050,6.5.1RC2.B060,6.5.1RC2.B070,6.5.1RC2.B080,6.5.1RC2.B090,6.5.RC2.B050,8.0.0,8.0.0-LCND81,8.0.0.SPC100,8.0.1,8.0.RC2,8.0.RC3,8.0.RC3.B041,8.0.RC3.SPC100;</p> <p>NFV_FusionSphere versions</p> <p>6.5.1.SPC23,8.0.0.SPC12;</p> <p>SMC2.0 versions</p>	<p>https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-02-privilege-en</p>	H-HUA-SMC2-160221/1137
-------------------------------	-----------	-----	---	--	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V600R019C00,V600R019C10 ; iMaster MAE-M versions MAE-TOOL(FusionSphereBasicTemplate_Euler_X86)V100R020C10SPC220. CVE ID : CVE-2021-22299		
ecns280_td					
Cleartext Storage of Sensitive Information	06-Feb-21	1.9	There is an information leak vulnerability in eCNS280_TD versions V100R005C00 and V100R005C10. A command does not have timeout exit mechanism. Temporary file contains sensitive information. This allows attackers to obtain information by inter-process access that requires other methods. CVE ID : CVE-2021-22300	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-cgp-en	H-HUA-ECNS-160221/1138
taurus-al00a					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Feb-21	5	Some Huawei products have an inconsistent interpretation of HTTP requests vulnerability. Attackers can exploit this vulnerability to cause information leak. Affected product versions include: CampusInsight versions V100R019C10; ManageOne versions 6.5.1.1, 6.5.1.SPC100, 6.5.1.SPC200, 6.5.1RC1, 6.5.1RC2, 8.0.RC2. Affected product versions include: Taurus-AL00A versions 10.0.0.1(C00E1R1P1).	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210120-01-http-en	H-HUA-TAUR-160221/1139

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-22293		
Out-of-bounds Read	06-Feb-21	3.6	There is an out-of-bound read vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module does not verify the some input. Attackers can exploit this vulnerability by sending malicious input through specific app. This could cause out-of-bound, compromising normal service. CVE ID : CVE-2021-22302	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-smartphone-en	H-HUA-TAUR-160221/1140
Double Free	06-Feb-21	4.3	There is a pointer double free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). There is a lack of muti-thread protection when a function is called. Attackers can exploit this vulnerability by performing malicious operation to cause pointer double free. This may lead to module crash, compromising normal service. CVE ID : CVE-2021-22303	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-02-smartphone-en	H-HUA-TAUR-160221/1141
Use After Free	06-Feb-21	2.1	There is a use after free vulnerability in Taurus-AL00A 10.0.0.1(C00E1R1P1). A module may refer to some memory after it has been freed while dealing with some messages. Attackers can exploit this vulnerability by sending specific message to the affected module. This may lead to module crash, compromising normal service.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-03-smartphone-en	H-HUA-TAUR-160221/1142

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-22304		
mate_30					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Feb-21	4.6	Mate 30 10.0.0.203(C00E201R7P2) have a buffer overflow vulnerability. After obtaining the root permission, an attacker can exploit the vulnerability to cause buffer overflow. CVE ID : CVE-2021-22301	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-01-buffer-en	H-HUA-MATE-160221/1143
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Feb-21	2.1	There is a buffer overflow vulnerability in Mate 30 10.1.0.126(C00E125R5P3). A module does not verify the some input when dealing with messages. Attackers can exploit this vulnerability by sending malicious input through specific module. This could cause buffer overflow, compromising normal service. CVE ID : CVE-2021-22305	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-04-smartphone-en	H-HUA-MATE-160221/1144
Out-of-bounds Read	06-Feb-21	2.1	There is an out-of-bound read vulnerability in Mate 30 10.0.0.182(C00E180R6P2). A module does not verify the some input when dealing with messages. Attackers can exploit this vulnerability by sending malicious input through specific module. This could cause out-of-bound, compromising normal service. CVE ID : CVE-2021-22306	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-05-smartphone-en	H-HUA-MATE-160221/1145
Not Available	06-Feb-21	2.1	There is a weak algorithm	https://www	H-HUA-

CVSS Scoring Scale	0-1	1-2	2-3	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 in Mate 3010.0.0.203(C00E201R7P2). The protection is insufficient for the modules that should be protected. Local attackers can exploit this vulnerability to affect the integrity of certain module. CVE ID : CVE-2021-22307	.huawei.com/en/psirt/security-advisories/huawei-sa-20210127-06-smartphone-en	MATE-160221/1146

LG

wing

Not Available	04-Feb-21	7.5	An issue was discovered on LG Wing mobile devices with Android OS 10 software. The biometric sensor has weak security properties. The LG ID is LVE-SMP-200030 (February 2021). CVE ID : CVE-2021-26688	https://lgsecurity.lge.com/	H-LG-WING-160221/1147
---------------	-----------	-----	--	---	-----------------------

Logitech

lan-w300n\pgrb

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-21	7.7	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors. CVE ID : CVE-2021-20638	https://www.elecom.co.jp/news/security/20210126-01/	H-LOG-LAN--160221/1148
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-Feb-21	7.7	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors. CVE ID : CVE-2021-20639	https://www.elecom.co.jp/news/security/20210126-01/	H-LOG-LAN--160221/1149

CVSS Scoring Scale	0-1	1-2	2-3	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')					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Feb-21	7.7	Buffer overflow vulnerability in LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute an arbitrary OS command via unspecified vectors. CVE ID : CVE-2021-20640	https://www.elecom.co.jp/news/security/20210126-01/	H-LOG-LAN--160221/1150

Siemens

scalance_w780

Allocation of Resources Without Limits or Throttling	09-Feb-21	3.3	A vulnerability has been identified in SCALANCE W780 and W740 (IEEE 802.11n) family (All versions < V6.3). Sending specially crafted packets through the ARP protocol to an affected device could cause a partial denial-of-service, preventing the device to operate normally for a short period of time. CVE ID : CVE-2021-25666	https://certportal.siemens.com/productcert/pdf/sa-686152.pdf	H-SIE-SCAL-160221/1151
--	-----------	-----	--	---	------------------------

scalance_w740

Allocation of Resources Without Limits or Throttling	09-Feb-21	3.3	A vulnerability has been identified in SCALANCE W780 and W740 (IEEE 802.11n) family (All versions < V6.3). Sending specially crafted packets through the ARP protocol to an affected device could cause a partial denial-of-service, preventing the device to operate normally for a short period of time. CVE ID : CVE-2021-25666	https://certportal.siemens.com/productcert/pdf/sa-686152.pdf	H-SIE-SCAL-160221/1152
--	-----------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sonicwall					
sma_200					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	H-SON-SMA_160221/1153
sma_210					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	H-SON-SMA_160221/1154
sma_400					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	H-SON-SMA_160221/1155

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sma_410					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	H-SON-SMA_-160221/1156
sma_100					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Feb-21	7.5	A SQL-Injection vulnerability in the SonicWall SSLVPN SMA100 product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information. This vulnerability impacts SMA100 build version 10.x. CVE ID : CVE-2021-20016	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001	H-SON-SMA_-160221/1157

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