



CVE-2020-3357

Published on: 07/16/2020 12:00:00 AM UTC

Last Modified on: 08/06/2021 06:46:00 PM UTC

CVE-2020-3357 - advisory for cisco-sa-sb-rce-dos-9ZAjx4

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Rv340w Dual Wan Gigabit Wireless-ac Vpn Router](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability

exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition.

CVE-2020-3357 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **CRITICAL** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Small Business RV Series Router Firmware** version **n/a**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact	Impact	Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers SSL Remote Code Execution and Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	 CISCO 20200715 Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers SSL Remote Code Execution and Denial of Service Vulnerability
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Cisco	Rv340w Dual Wan Gigabit Wireless-ac Vpn Router	-	All	All	All
Hardware  	Cisco	Rv340w Dual Wan Gigabit Wireless-ac Vpn Router	-	All	All	All
Operating System	Cisco	Rv340w Dual Wan Gigabit Wireless-ac Vpn Router Firmware	All	All	All	All
Operating System	Cisco	Rv340w Dual Wan Gigabit Wireless-ac Vpn Router Firmware	All	All	All	All
Hardware  	Cisco	Rv340 Dual Wan Gigabit Vpn Router	-	All	All	All
Hardware  	Cisco	Rv340 Dual Wan Gigabit Vpn Router	-	All	All	All
Operating System	Cisco	Rv340 Dual Wan Gigabit Vpn Router Firmware	All	All	All	All
Operating System	Cisco	Rv340 Dual Wan Gigabit Vpn Router Firmware	All	All	All	All
Hardware  	Cisco	Rv345p Dual Wan Gigabit Poe Vpn Router	-	All	All	All
Hardware  	Cisco	Rv345p Dual Wan Gigabit Poe Vpn Router	-	All	All	All
Operating System	Cisco	Rv345p Dual Wan Gigabit Poe Vpn Router Firmware	All	All	All	All
Operating System	Cisco	Rv345p Dual Wan Gigabit Poe Vpn Router Firmware	All	All	All	All
Hardware  	Cisco	Rv345 Dual Wan Gigabit Vpn Router	-	All	All	All
Hardware  	Cisco	Rv345 Dual Wan Gigabit Vpn Router	-	All	All	All
Operating System	Cisco	Rv345 Dual Wan Gigabit Vpn Router Firmware	All	All	All	All
Operating System	Cisco	Rv345 Dual Wan Gigabit Vpn Router Firmware	All	All	All	All

cpe:2.3:h:cisco:rv340w_dual_wan_gigabit_wireless-ac_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:rv340w_dual_wan_gigabit_wireless-ac_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv340w_dual_wan_gigabit_wireless-ac_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv340w_dual_wan_gigabit_wireless-ac_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:rv340_dual_wan_gigabit_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:rv340_dual_wan_gigabit_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv340_dual_wan_gigabit_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv340_dual_wan_gigabit_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:rv345p_dual_wan_gigabit_poe_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:rv345p_dual_wan_gigabit_poe_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv345p_dual_wan_gigabit_poe_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv345p_dual_wan_gigabit_poe_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:rv345_dual_wan_gigabit_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:rv345_dual_wan_gigabit_vpn_router:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv345_dual_wan_gigabit_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:rv345_dual_wan_gigabit_vpn_router_firmware:*~::~~::~~::~~::~~::~~:::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report