



CVE-2021-1157

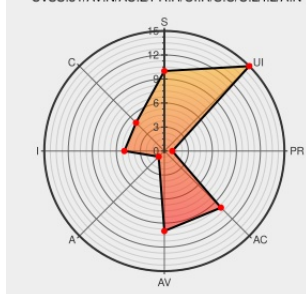
Published on: 01/13/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:55 PM UTC

CVE-2021-1157 - advisory for cisco-sa-rv-stored-xss-LPTQ3EQC

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

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



Certain versions of [Application Extension Platform](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. The vulnerabilities are due to insufficient input validation by the web-based

management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device.

CVE-2021-1157 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

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

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

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact				
NONE	PARTIAL	NONE				
CVE References						
Description	Tags	Link				
Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface Stored Cross-Site Scripting Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20210113 Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface Stored Cross-Site Scripting Vulnerabilities				
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
Application	Cisco	Application Extension Platform	1.0.3.55	All	All	All
Application	Cisco	Application Extension Platform	1.0.3.55	All	All	All
Hardware 	Cisco	Rv110w	-	All	All	All
Hardware 	Cisco	Rv110w	-	All	All	All
Hardware 	Cisco	Rv110w	-	All	All	All
Operating System	Cisco	Rv110w Firmware	1.2.2.8	All	All	All
Operating System	Cisco	Rv110w Firmware	1.3.1.7	All	All	All
Operating System	Cisco	Rv110w Firmware	1.2.2.8	All	All	All
Operating System	Cisco	Rv110w Firmware	1.3.1.7	All	All	All
Hardware 	Cisco	Rv130w	-	All	All	All
Hardware 	Cisco	Rv130w	-	All	All	All
Hardware 	Cisco	Rv130w	-	All	All	All
Operating System	Cisco	Rv130w Firmware	1.2.2.8	All	All	All
Operating System	Cisco	Rv130w Firmware	1.3.1.7	All	All	All
Operating System	Cisco	Rv130w Firmware	1.2.2.8	All	All	All
Operating System	Cisco	Rv130w Firmware	1.3.1.7	All	All	All

cpe:2.3:o:cisco:rv130w_firmware:1.2.2.8:*****:
cpe:2.3:o:cisco:rv130w_firmware:1.3.1.7:*****:
cpe:2.3:o:cisco:rv130w_firmware:1.2.2.8:*****:
cpe:2.3:o:cisco:rv130w_firmware:1.3.1.7:*****:
cpe:2.3:h:cisco:rv130_vpn_router:-:*****:
cpe:2.3:h:cisco:rv130_vpn_router:-:*****:
cpe:2.3:h:cisco:rv130_vpn_router:-:*****:
cpe:2.3:o:cisco:rv130_vpn_router_firmware:1.2.2.8:*****:
cpe:2.3:o:cisco:rv130_vpn_router_firmware:1.3.1.7:*****:
cpe:2.3:o:cisco:rv130_vpn_router_firmware:1.2.2.8:*****:
cpe:2.3:o:cisco:rv130_vpn_router_firmware:1.3.1.7:*****:
cpe:2.3:h:cisco:rv215w_wireless-n_vpn_router:-:*****:
cpe:2.3:h:cisco:rv215w_wireless-n_vpn_router:-:*****:
cpe:2.3:h:cisco:rv215w_wireless-n_vpn_router:-:*****:
cpe:2.3:o:cisco:rv215w_wireless-n_vpn_router_firmware:1.2.2.8:*****:
cpe:2.3:o:cisco:rv215w_wireless-n_vpn_router_firmware:1.3.1.7:*****:
cpe:2.3:o:cisco:rv215w_wireless-n_vpn_router_firmware:1.2.2.8:*****:
cpe:2.3:o:cisco:rv215w_wireless-n_vpn_router_firmware:1.3.1.7:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)