



# CVE-2021-1207

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

Last Modified on: 11/07/2023 03:27:00 AM UTC

## CVE-2021-1207 - advisory for cisco-sa-rv-overflow-WUnUgv4U

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

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



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 execute arbitrary code or cause an affected device to restart unexpectedly. The vulnerabilities are due to improper validation of user-supplied input in

the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition. To exploit these vulnerabilities, an attacker would need to have valid administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.

CVE-2021-1207 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

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

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

CVSS3 Score: **7.2 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>HIGH</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **9 - HIGH**

| Access Vector | Access Complexity | Authentication |
|---------------|-------------------|----------------|
|---------------|-------------------|----------------|

|                        |                  |                     |
|------------------------|------------------|---------------------|
| NETWORK                | LOW              | SINGLE              |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| COMPLETE               | COMPLETE         | COMPLETE            |

### CVE References

| Description                                                                                                                   | Tags                                                                                            | Link                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerabilities | <a href="#">Vendor Advisory</a><br><a href="#">tools.cisco.com</a><br><a href="#">text/html</a> | <a href="#">CISCO 20210113 Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface Remote Command Execution and Denial of Service Vulnerabilities</a> |

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](mailto: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  | <a href="#">Application Extension Platform</a> | 1.0.3.55 | All    | All     | All      |
| Application                                                                                  | Cisco  | <a href="#">Application Extension Platform</a> | 1.0.3.55 | All    | All     | All      |
| Hardware  | Cisco  | <a href="#">Rv110w</a>                         | -        | All    | All     | All      |
| Hardware  | Cisco  | <a href="#">Rv110w</a>                         | -        | All    | All     | All      |
| Hardware  | Cisco  | <a href="#">Rv110w</a>                         | -        | All    | All     | All      |
| Operating System                                                                             | Cisco  | <a href="#">Rv110w Firmware</a>                | 1.2.2.8  | All    | All     | All      |
| Operating System                                                                             | Cisco  | <a href="#">Rv110w Firmware</a>                | 1.3.1.7  | All    | All     | All      |
| Operating System                                                                             | Cisco  | <a href="#">Rv110w Firmware</a>                | 1.2.2.8  | All    | All     | All      |
| Operating System                                                                             | Cisco  | <a href="#">Rv110w Firmware</a>                | 1.3.1.7  | All    | All     | All      |
| Hardware  | Cisco  | <a href="#">Rv130w</a>                         | -        | All    | All     | All      |
| Hardware  | Cisco  | <a href="#">Rv130w</a>                         | -        | All    | All     | All      |
| Hardware  | Cisco  | <a href="#">Rv130w</a>                         | -        | All    | All     | All      |
| Operating System                                                                             | Cisco  | <a href="#">Rv130w Firmware</a>                | 1.2.2.8  | All    | All     | All      |
| Operating System                                                                             | Cisco  | <a href="#">Rv130w Firmware</a>                | 1.3.1.7  | All    | All     | All      |
| Operating System                                                                             | Cisco  | <a href="#">Rv130w Firmware</a>                | 1.2.2.8  | All    | All     | All      |

|                                                                                            |       |                                       |         |     |     |     |
|--------------------------------------------------------------------------------------------|-------|---------------------------------------|---------|-----|-----|-----|
|                                                                                            |       |                                       |         |     |     |     |
| Operating System                                                                           | Cisco | Rv130w Firmware                       | 1.3.1.7 | All | All | All |
| Hardware  | Cisco | Rv130 Vpn Router                      | -       | All | All | All |
| Hardware  | Cisco | Rv130 Vpn Router                      | -       | All | All | All |
| Hardware  | Cisco | Rv130 Vpn Router                      | -       | All | All | All |
| Operating System                                                                           | Cisco | Rv130 Vpn Router Firmware             | 1.2.2.8 | All | All | All |
| Operating System                                                                           | Cisco | Rv130 Vpn Router Firmware             | 1.3.1.7 | All | All | All |
| Operating System                                                                           | Cisco | Rv130 Vpn Router Firmware             | 1.2.2.8 | All | All | All |
| Operating System                                                                           | Cisco | Rv130 Vpn Router Firmware             | 1.3.1.7 | All | All | All |
| Hardware  | Cisco | Rv215w Wireless-n Vpn Router          | -       | All | All | All |
| Hardware  | Cisco | Rv215w Wireless-n Vpn Router          | -       | All | All | All |
| Hardware  | Cisco | Rv215w Wireless-n Vpn Router          | -       | All | All | All |
| Operating System                                                                           | Cisco | Rv215w Wireless-n Vpn Router Firmware | 1.2.2.8 | All | All | All |
| Operating System                                                                           | Cisco | Rv215w Wireless-n Vpn Router Firmware | 1.3.1.7 | All | All | All |
| Operating System                                                                           | Cisco | Rv215w Wireless-n Vpn Router Firmware | 1.2.2.8 | All | All | All |
| Operating System                                                                           | Cisco | Rv215w Wireless-n Vpn Router Firmware | 1.3.1.7 | All | All | All |
| cpe:2.3:a:cisco:application_extension_platform:1.0.3.55:*:*:*:*:*:                         |       |                                       |         |     |     |     |
| cpe:2.3:a:cisco:application_extension_platform:1.0.3.55:*:*:*:*:*:                         |       |                                       |         |     |     |     |
| cpe:2.3:h:cisco:rv110w:-:*:*:*:*:*:                                                        |       |                                       |         |     |     |     |
| cpe:2.3:h:cisco:rv110w:-:*:*:*:*:*:                                                        |       |                                       |         |     |     |     |
| cpe:2.3:h:cisco:rv110w:-:*:*:*:*:*:                                                        |       |                                       |         |     |     |     |
| cpe:2.3:o:cisco:rv110w_firmware:1.2.2.8:*:*:*:*:*:                                         |       |                                       |         |     |     |     |
| cpe:2.3:o:cisco:rv110w_firmware:1.3.1.7:*:*:*:*:*:                                         |       |                                       |         |     |     |     |
| cpe:2.3:o:cisco:rv110w_firmware:1.2.2.8:*:*:*:*:*:                                         |       |                                       |         |     |     |     |
| cpe:2.3:o:cisco:rv110w_firmware:1.3.1.7:*:*:*:*:*:                                         |       |                                       |         |     |     |     |
| cpe:2.3:h:cisco:rv130w:-:*:*:*:*:*:                                                        |       |                                       |         |     |     |     |
| cpe:2.3:h:cisco:rv130w:-:*:*:*:*:*:                                                        |       |                                       |         |     |     |     |
|                                                                                            |       |                                       |         |     |     |     |

