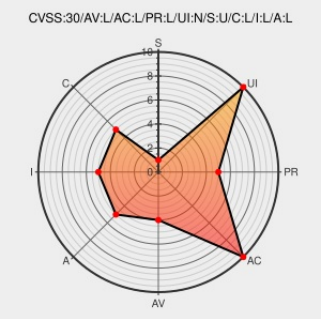
# CVE-2019-1816

Published on: 05/03/2019 12:00:00 AM UTC

Last Modified on: 03/24/2023 06:14:00 PM UTC

**CVE-2019-1816** - advisory for cisco-sa-20190501-wsa-privesc

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Web Security Appliance from Cisco contain the following vulnerability:

A vulnerability in the log subscription subsystem of the Cisco Web Security Appliance (WSA) could allow an authenticated, local attacker to perform command injection and elevate privileges to root. The vulnerability is due to insufficient validation of user-supplied input on the web and command-line interface. An attacker could exploit this vulnerability by authenticating to the affected device and injecting scripting commands in the scope of the log subscription subsystem. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root.

CVE-2019-1816 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 vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Web Security Appliance (WSA)** version **10.1.4-017**

Affected Vendor/Software: **Cisco** - **Cisco Web Security Appliance (WSA)** version **10.5.4-018**

Affected Vendor/Software: **Cisco** - **Cisco Web Security Appliance (WSA)** version **11.5.2-020**

Affected Vendor/Software: **Cisco** - **Cisco Web Security Appliance (WSA)** version **11.7.0-406**

CVSS3 Score: 7.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

CVSS2 Score: 7.2 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Cisco Web Security Appliance Privilege Escalation Vulnerability | Vendor Advisory<br>tools.cisco.com<br>text/html | CISCO 20190501 Cisco Web Security Appliance Privilege Escalation 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 |
|---|---|---|---|---|---|---|
| Application | Cisco | Web Security Appliance | 10.5.2-072 | All | All | All |
| Application | Cisco | Web Security Appliance | 11.0.0-641 | All | All | All |
| Application | Cisco | Web Security Appliance | 11.5.0-fcs-614 | All | All | All |
| Application | Cisco | Web Security Appliance | wsa10.5.0-fcs-000 | All | All | All |
| Application | Cisco | Web Security Appliance | 10.5.2-072 | All | All | All |
| Application | Cisco | Web Security Appliance | 11.0.0-641 | All | All | All |
| Application | Cisco | Web Security Appliance | 11.5.0-fcs-614 | All | All | All |
| Application | Cisco | Web Security Appliance | wsa10.5.0-fcs-000 | All | All | All |

cpe:2.3:a:cisco:web_security_appliance:10.5.2-072:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:web_security_appliance:11.0.0-641:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:web_security_appliance:11.5.0-fcs-614:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:web_security_appliance:wsa10.5.0-fcs-000:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:web_security_appliance:10.5.2-072:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:web_security_appliance:11.0.0-641:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:web_security_appliance:11.5.0-fcs-614:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:web_security_appliance:wsa10.5.0-fcs-000:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→



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