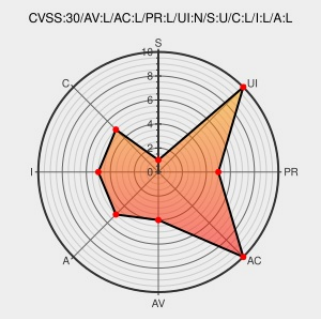
CVE-2020-3367

Published on: 11/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:38 PM UTC

CVE-2020-3367 - advisory for cisco-sa-wsa-prv-esc-nPzWZrQj

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



Certain versions of Asyncos from Cisco contain the following vulnerability:

A vulnerability in the log subscription subsystem of Cisco AsyncOS for the Cisco Secure Web Appliance (formerly Web Security Appliance) could allow an authenticated, local attacker to perform command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the web interface and CLI. 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-2020-3367 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 **n/a**

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	**Integrity**	**Availability**

Impact	Impact	Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco Secure Web Appliance Privilege Escalation Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201118 Cisco Secure Web 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
Operating System	Cisco	Asyncos	All	All	All	All
Operating System	Cisco	Asyncos	All	All	All	All

cpe:2.3:o:cisco:asyncos:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:asyncos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→