



CVE-2019-15266

Published on: 10/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

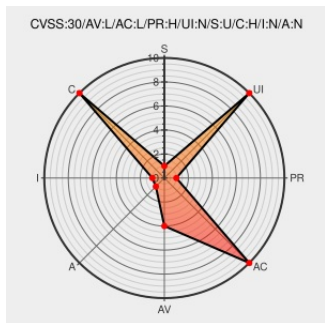
CVE-2019-15266 - advisory for cisco-sa-20191016-wlc-pathtrav

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Wireless Lan Controller Software](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the CLI of Cisco Wireless LAN Controller (WLC) Software could allow an authenticated, local attacker to view system files that should be restricted. This vulnerability is due to improper sanitization of user-supplied input in command-line parameters that describe filenames. An attacker could exploit this vulnerability by using directory traversal techniques to submit a path to a desired file location. A successful exploit could allow the attacker to view system files that may contain sensitive information.

CVE-2019-15266 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 vulnerability that is described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco Wireless LAN Controller (WLC)** version n/a

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Cisco Wireless LAN Controller Path Traversal Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20191016 Cisco Wireless LAN Controller Path Traversal 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	Wireless Lan Controller Software	All	All	All	All
Application	Cisco	Wireless Lan Controller Software	All	All	All	All

cpe:2.3:a:cisco:wireless_lan_controller_software:*:*:*:*:*:

cpe:2.3:a:cisco:wireless_lan_controller_software:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→