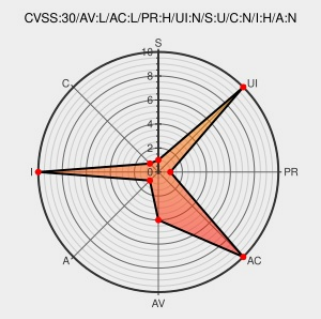
# CVE-2020-3476

Published on: 09/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

**CVE-2020-3476** - advisory for cisco-sa-file-overwrite-Ynu5PrJD

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




Certain versions of Ios from Cisco contain the following vulnerability:

A vulnerability in the CLI implementation of a specific command of Cisco IOS XE Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying host file system. The vulnerability is due to insufficient validation of the parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of any arbitrary file that resides on the underlying host file system.

CVE-2020-3476 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 IOS XE Software** version **n/a**

CVSS3 Score: 6 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

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

## CVE References

| Description | Tags | Link |
|---|---|---|
| Cisco IOS XE Software Arbitrary File Overwrite Vulnerability | Vendor Advisory<br>tools.cisco.com<br>text/html | CISCO 20200924 Cisco IOS XE Software Arbitrary File Overwrite Vulnerability |



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 | Ios | 16.10.1 | All | All | All |
| Operating System | Cisco | Ios | 16.9 | All | All | All |
| Operating System | Cisco | Ios | 16.10.1 | All | All | All |
| Operating System | Cisco | Ios | 16.9 | All | All | All |

cpe:2.3:o:cisco:ios:16.10.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:16.9:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:16.10.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:16.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→