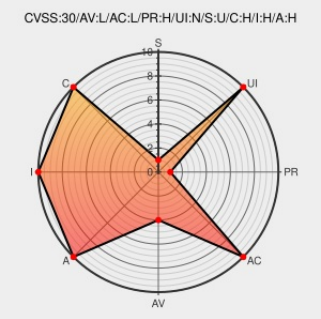
CVE-2018-15376

Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:27 PM UTC

CVE-2018-15376 - advisory for cisco-sa-20180926-ir800-memwrite

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



Certain versions of Ios from Cisco contain the following vulnerability:

A vulnerability in the embedded test subsystem of Cisco IOS Software for Cisco 800 Series Industrial Integrated Services Routers could allow an authenticated, local attacker to write arbitrary values to arbitrary locations in the memory space of an affected device. The vulnerability is due to the presence of certain test commands that were intended to be available only in internal development builds of the affected software. An attacker could exploit this vulnerability by using these commands on an affected device. A successful exploit could allow the attacker to write arbitrary values to arbitrary locations in the memory space of the affected device.

CVE-2018-15376 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Cisco** - **Cisco IOS Software** version **n/a**

CVSS3 Score: 6.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	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

CVE References

Description	Tags	Link
Cisco IOS Software for Cisco 800 Series Industrial Integrated Services Routers Arbitrary Memory Write Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20180926 Cisco IOS Software for Cisco 800 Series Industrial Integrated Services Routers Arbitrary Memory Write Vulnerabilities

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	Ios	15.5(2.21)t	All	All	All
Operating System	Cisco	Ios	15.5\(2.21\)t	All	All	All
Operating System	Cisco	Ios	15.6(3)m	All	All	All
Operating System	Cisco	Ios	15.6\(3\)m	All	All	All
Operating System	Cisco	Ios	15.5\(2.21\)t	All	All	All
Operating System	Cisco	Ios	15.6\(3\)m	All	All	All

cpe:2.3:o:cisco:ios:15.5(2.21)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.5\(2.21\)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.6(3)m:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.6\(3\)m:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.5\(2.21\)t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.6\(3\)m:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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