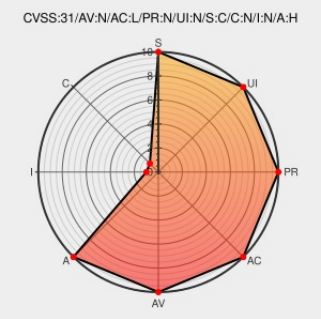
CVE-2018-15377

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

Last Modified on: 03/23/2021 11:24:28 PM UTC

CVE-2018-15377 - advisory for cisco-sa-20180926-pnp-memleak

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



Certain versions of Ios from Cisco contain the following vulnerability:

A vulnerability in the Cisco Network Plug and Play agent, also referred to as the Cisco Open Plug-n-Play agent, of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device. The vulnerability is due to insufficient input validation by the affected software. An attacker could exploit this vulnerability by sending invalid data to the Cisco Network Plug and Play agent on an affected device. A successful exploit could allow the attacker to cause a memory leak on the affected device, which could cause the device to reload.

CVE-2018-15377 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

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

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

CVE References

Description	Tags	Link
Rockwell Automation Stratix 5400/5410/5700 and ArmorStratix 5700 | CISA	Third Party Advisory US Government Resource ics-cert.us-cert.gov text/html	MISC ics-cert.us-cert.gov/advisories/ICSA-19-094-02
Cisco IOS and IOS XE Software Plug and Play Agent Memory Leak Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20180926 Cisco IOS and IOS XE Software Plug and Play Agent Memory Leak 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	Ios	15.7(3.1s)m	All	All	All
Operating System	Cisco	Ios	15.7\(3.1s\)m	All	All	All
Operating System	Cisco	Ios	denali-16.3.6	All	All	All
Operating System	Cisco	Ios	everest-16.5.1	All	All	All
Operating System	Cisco	Ios	15.7\(3.1s\)m	All	All	All
Operating System	Cisco	Ios	denali-16.3.6	All	All	All
Operating System	Cisco	Ios	everest-16.5.1	All	All	All

cpe:2.3:o:cisco:ios:15.7(3.1s)m:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.7\(3.1s\)m:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:denali-16.3.6:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:everest-16.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.7\(3.1s\)m:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:denali-16.3.6:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:everest-16.5.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→