



CVE-2018-0161

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-0161
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-28 22:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software running on certain n

Risk And Classification

EPSS: 0.009060000 probability, percentile 0.756950000 (date 2026-04-02)

CISA KEV: Listed on 2022-03-03; due 2022-03-17; ransomware use Unknown

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	IOS Software
Name	Cisco IOS Software Resource Management Errors Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-0161

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Catalyst 2960I-16ps-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-16ps-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-16ts-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-16ts-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-24pq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-24pq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-24ps-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-24ps-II	-	All	All	All

Hardware	Cisco	Catalyst 2960I-24tq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-24tq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-24ts-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-24ts-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48pq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48pq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48ps-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48ps-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48tq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48tq-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48ts-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-48ts-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-8ps-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-8ps-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-8ts-II	-	All	All	All
Hardware	Cisco	Catalyst 2960I-8ts-II	-	All	All	All
Hardware	Cisco	Catalyst Digital Building Series Switches-8p	-	All	All	All
Hardware	Cisco	Catalyst Digital Building Series Switches-8p	-	All	All	All
Hardware	Cisco	Catalyst Digital Building Series Switches-8u	-	All	All	All
Hardware	Cisco	Catalyst Digital Building Series Switches-8u	-	All	All	All
Operating System	Cisco	ios	15.2(5)e	All	All	All
Operating System	Cisco	ios	15.2(5)e	All	All	All
Operating System	Cisco	ios	15.2(5)e	All	All	All

References

Reference

103573

Cisco IOS Software Simple Network Management Protocol GET MIB Object ID Denial of Service Vulnerability

Cisco Catalyst 2960-L and Digital Building Series SNMP Processing Flaw Lets Remote Authenticated Users Cause the Target System to Relo

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)