



CVE-2018-0180

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-0180
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-28 22:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	Multiple vulnerabilities in the Login Enhancements (Login Block) feature of Cisco IOS Software could allow an unauthenticated user to bypass the login process and gain access to the device. The affected versions are Cisco IOS Software versions 1921, 1941, 1941w, and 2901. The affected versions are Cisco IOS Software versions 1921, 1941, 1941w, and 2901. The affected versions are Cisco IOS Software versions 1921, 1941, 1941w, and 2901. The affected versions are Cisco IOS Software versions 1921, 1941, 1941w, and 2901.

Risk And Classification

EPSS: 0.017340000 probability, percentile 0.823960000 (date 2026-04-01)

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 Denial-of-Service Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-0180

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	1921	-	All	All	All
Hardware	Cisco	1921	-	All	All	All
Hardware	Cisco	1941	-	All	All	All
Hardware	Cisco	1941	-	All	All	All
Hardware	Cisco	1941w	-	All	All	All
Hardware	Cisco	1941w	-	All	All	All
Hardware	Cisco	2901	-	All	All	All
Hardware	Cisco	2901	-	All	All	All

Hardware	Cisco	2911	-	All	All	All
Hardware	Cisco	2911	-	All	All	All
Hardware	Cisco	2921	-	All	All	All
Hardware	Cisco	2921	-	All	All	All
Hardware	Cisco	2951	-	All	All	All
Hardware	Cisco	2951	-	All	All	All
Hardware	Cisco	3925	-	All	All	All
Hardware	Cisco	3925	-	All	All	All
Hardware	Cisco	3925e	-	All	All	All
Hardware	Cisco	3925e	-	All	All	All
Hardware	Cisco	3945	-	All	All	All
Hardware	Cisco	3945	-	All	All	All
Hardware	Cisco	3945e	-	All	All	All
Hardware	Cisco	3945e	-	All	All	All
Hardware	Cisco	4451-x	-	All	All	All
Hardware	Cisco	4451-x	-	All	All	All
Operating System	Cisco	ios	All	All	All	All
Operating System	Cisco	ios	15.3(0.0.19)sy	All	All	All
Operating System	Cisco	ios	15.3\0.0.19\sy	All	All	All
Operating System	Cisco	ios	15.4(1)ia1.100	All	All	All
Operating System	Cisco	ios	15.4(2)t	All	All	All
Operating System	Cisco	ios	15.4(3)m	All	All	All
Operating System	Cisco	ios	15.4(3)m4.1	All	All	All
Operating System	Cisco	ios	15.4\1\ia1.100	All	All	All
Operating System	Cisco	ios	15.4\2\t	All	All	All
Operating System	Cisco	ios	15.4\3\m	All	All	All
Operating System	Cisco	ios	15.4\3\m4.1	All	All	All
Operating System	Cisco	ios	15.6(1.22)t	All	All	All
Operating System	Cisco	ios	15.6\1.22\t	All	All	All
Operating System	Cisco	ios	All	All	All	All
Operating System	Cisco	ios	15.3\0.0.19\sy	All	All	All
Operating System	Cisco	ios	15.4\1\ia1.100	All	All	All
Operating System	Cisco	ios	15.4\2\t	All	All	All
Operating System	Cisco	ios	15.4\3\m	All	All	All
Operating System	Cisco	ios	15.4\3\m4.1	All	All	All

Operating System	Cisco	ios	15.6(1.22)t	All	All	All
------------------	-------	-----	-------------	-----	-----	-----

References

Reference	Source	Link	Tags
Cisco IOS Software Login Enhancements Login Block Denial of Service Vulnerabilities	CONFIRM	tools.cisco.com	Mitigation, Ve
Malformed Request	BID	www.securityfocus.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

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