

CVE-2018-0179

Cisco IOS Software Denial-of-Service Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Multiple vulnerabilities in the Login Enhancements (Login Block) feature of Cisco IOS Software could allow an unauthenticated, remote attacker to trigger a reload of an affected system, resulting in a denial of service (DoS) condition. These vulnerabilities affect Cisco devices that are running Cisco IOS Software Release 15.4(2)T, 15.4(3)M, or 15.4(2)CG and later. Cisco Bug IDs: CSCuy32360, CSCuz60599.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 5.9 Medium · NVD	EPSS 0.049 92.1st percentile · FIRST	CISA DEADLINE Mar 17, 2022 KEV since 2022 · listed over a year
--	---	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.049 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.9	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 291 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ios	15.3\(\00.00.19\)sy 15.4\(\01\)ia001.100 15.6\(\01.22\)t 15.4\(\03\)m4.1 15.4\(\2\)cg 15.4\(\2\)t 15.4\(\3\)m	no fixed version listed	NVD
3925 integrated services router	—	no fixed version listed	NVD
3925e integrated services router	—	no fixed version listed	NVD
3945 integrated services router	—	no fixed version listed	NVD
3945e integrated services router	—	no fixed version listed	NVD
1000 integrated services router	—	no fixed version listed	NVD
1100-4g\6g integrated services router	—	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
1100-4g integrated services router	–	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-xmxh-qgmj-jcc4

Additional guidance tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-slogin

NVD nvd.nist.gov/vuln/detail/CVE-2018-0179

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-1002

Current data evalnable.com/vulnerability-management/cve/CVE-2018-0179

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.