CVE-2006-0486

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-0486
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-01 02:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Certain Cisco IOS releases in 12.2S based trains with maintenance release number 25 and later, 12.3T based trains, and 1

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:P/A:P

EPSS: 0.000990000 probability, percentile 0.275210000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Operating System	Cisco	Ios	12.2\(25\)s	All	All	All
Operating System	Cisco	Ios	12.3t	All	All	All
Operating System	Cisco	Ios	12.4	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
SecurityTracker.com Archives - Cisco IOS AAA Command Authorization Feature May Let Remote Authenticated Users Gain Elevated Privileg
IBM X-Force Exchange
Repository / Oval Repository
www.osvdb.org/22723
Cisco - Networking, Cloud, and Cybersecurity Solutions
Cisco IOS AAA Command Authentication Bypass Vulnerability - Advisories - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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