CVE-2011-0946

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

Summary

CVE	CVE-2011-0946
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-10-03 23:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The NAT implementation in Cisco IOS 12.1 through 12.4 and 15.0 through 15.1, and IOS XE 3.1.xSG, allows remote attack

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	All	All	All	All

Operating System	Cisco	Ios	All	All	All	All
Operating System	Cisco	Ios Xe	3.1.0sg	All	All	All
Operating System	Cisco	Ios Xe	3.1.1sg	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Cisco Security Advisory: Cisco IOS Software Network Address Translation Vulnerabilities - Cisco Systems	af854a3a-2127-42
Cisco IOS Software NetMeeting Directory LDAP Network Address Translation Processing Denial of Service Vulnerability	af854a3a-2127-42
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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