CVE-2014-0660

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

Summary

CVE	CVE-2014-0660
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-22 21:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cisco TelePresence ISDN Gateway with software before 2.2(1.92) allows remote attackers to cause a denial of service (D-

Risk And Classification

Primary CVSS: v2.0 7.1 from nvd@nist.gov

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

EPSS: 0.015130000 probability, percentile 0.813000000 (date 2026-05-03)

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Cisco	Telepresence Isdn Gateway Software	2.1\(1.43\)	All	All	All
Application	Cisco	Telepresence Isdn Gateway Software	2.1\(1.49\)	All	All	All
Application	Cisco	Telepresence Isdn Gateway Software	2.1\(1.56\)	All	All	All
Application	Cisco	Telepresence Isdn Gateway Software	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Security Advisory SA56591 - Cisco TelePresence ISDN Gateway Q.931 STATUS Packets Processing Denial of Service Vulnerability - Secuni
Alert Details - Security Center - Cisco Systems
Cisco TelePresence ISDN Gateway D-channel Denial of Service Vulnerability
osvdb.org/102361
Cisco TelePresence ISDN Gateway D-Channel Denial of Service Vulnerability
IBM X-Force Exchange
Cisco TelePresence ISDN Gateway Q.931 Processing Flaw Lets Remote Users Deny Service - SecurityTracker
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.