CVE-2007-4291

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

Summary

CVE	CVE-2007-4291
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-09 21:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Cisco IOS 12.0 through 12.4 allows remote attackers to cause a denial of service via (1) a malformed MGCP packet, which

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

Problem Types: NVD-CWE-Other | 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
Operating System	Cisco	Ios	12.0	All	All	All

Operating System	Cisco	Ios	12.1	All	All	All
Operating System	Cisco	Ios	12.2	All	All	All
Operating System	Cisco	Ios	12.3	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	S
osvdb.org/36679	af
osvdb.org/36678	af
Repository / Oval Repository	af
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af
IBM X-Force Exchange	af
IBM X-Force Exchange	af
IBM X-Force Exchange	af
Cisco Security Advisory: Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager - Cisco Systems	af
osvdb.org/36677	af
SecurityTracker.com Archives - Cisco IOS Bugs in Voice Services Let Remote Users Deny Service or Potentially Execute Arbitrary Code	af
Cisco IOS and Unified Communications Manager Multiple Voice Vulnerabilities	af
osvdb.org/36681	af
Cisco IOS Voice Service Multiple Protocol Handling Vulnerabilities - Advisories - Secunia	af
osvdb.org/36680	af
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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