



CVE-2004-1464

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2004-1464
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2026-04-16 14:03:22 UTC
Description	Cisco IOS 12.2(15) and earlier allows remote attackers to cause a denial of service (refused VTY (virtual terminal) connecti

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from nvd@nist.gov

CVSS: 3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.024110000 probability, percentile 0.851440000 (date 2026-04-23)

CISA KEV: Listed on 2023-05-19; due 2023-06-09; ransomware use Unknown

Problem Types: CWE-400 | n/a | CWE-400 CWE-400 Uncontrolled Resource Consumption

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	IOS
Name	Cisco IOS Denial-of-Service Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet ; https://nvd.nist.gov/vuln/detail/CVE-2004-1464

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

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

References

Reference

Cisco - Networking, Cloud, and Cybersecurity Solutions

Cisco IOS Telnet and Reverse Telnet TCP Bug Lets Remote Users Deny Subsequent Management Terminal Connections - SecurityTracker

VU#384230 - Cisco IOS fails to properly handle telnet connections

www.cisa.gov/known-exploited-vulnerabilities-catalog

Cisco IOS Telnet Service Remote Denial of Service Vulnerability

Secunia - Advisories - Cisco IOS Telnet Service Denial of Service Vulnerability

IBM X-Force Exchange

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2023-05-19T00:00:00.000Z	CVE-2004-1464 added to CISA KEV

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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