

# CVE-2004-1464

## Cisco IOS Denial-of-Service Vulnerability

CISA KEV since May 19, 2023

Actively exploited

Cisco IOS 12.2(15) and earlier allows remote attackers to cause a denial of service (refused VTY (virtual terminal) connections), via a crafted TCP connection to the Telnet or reverse Telnet port.

|                                                                     |                                                |                                                        |                                                                                   |
|---------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>EVRS</b><br><b>75</b> / <sub>100</sub><br><b>Urgent</b> priority | <b>CVSS V3.1</b><br><b>5.9</b><br>Medium · NVD | <b>EPSS</b><br><b>0.048</b><br>92nd percentile · FIRST | <b>CISA DEADLINE</b><br><b>Jun 9, 2023</b><br>KEV since 2023 · listed over a year |
|---------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                            |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.048 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 5.9                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** No patch reported by the connected remediation source

**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE | AFFECTED      | FIXED IN          | SOURCE |
|---------|---------------|-------------------|--------|
| ios     | ≤ 12.2\15\zj3 | after 12.2\15\zj3 | NVD    |

### Sources

|                                |                                                                                                                                                                                                                     |                   |                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>sec.cloudapps.cisco.com</b> | <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet">sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet</a> | <b>NVD</b>        | <a href="https://nvd.nist.gov/vuln/detail/CVE-2004-1464">nvd.nist.gov/vuln/detail/CVE-2004-1464</a>                       |
| <b>CISA KEV</b>                | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                                                                                             | <b>ENISA EUVD</b> | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2004-1458">euvd.enisa.europa.eu/vulnerability/EUVD-2004-1458</a> |
| <b>Current data</b>            | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2004-1464">evulnable.com/vulnerability-management/cve/CVE-2004-1464</a>                                                                             |                   |                                                                                                                           |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.