



# CVE-2011-3289

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

## Summary

|                 |                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2011-3289                                                                                                         |
| State           | PUBLISHED                                                                                                             |
| Assigner        | cisco                                                                                                                 |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                          |
| Published       | 2012-05-02 10:09:21 UTC                                                                                               |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                               |
| Description     | Cisco IOS 12.4 and 15.0 through 15.2 allows physically proximate attackers to bypass the No Service Password-Recovery |

## Risk And Classification

Primary CVSS: v2.0 3.6 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---------|---------|--------|---------|----------|
| Operating System | Cisco  | ios     | 12.4    | All    | All     | All      |

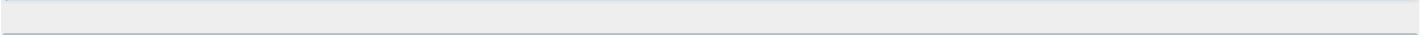
|                  |       |     |      |     |     |     |
|------------------|-------|-----|------|-----|-----|-----|
| Operating System | Cisco | ios | 15.0 | All | All | All |
| Operating System | Cisco | ios | 15.1 | All | All | All |
| Operating System | Cisco | ios | 15.2 | All | All | All |

Vendor Declared Affected Products

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

References

| Reference                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------|
| Cross-Platform Release Notes for Cisco IOS Release 15.1M&T - Release 15.1(2)T Caveats [Cisco IOS 15.1M&T] - Cisco Systems                  |
| Cisco IOS Multiple Bugs Let Remote Users Bypass Security Controls, Obtain Potentially Sensitive Information, and Deny Service - SecurityTr |
| 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.