



# CVE-2012-3291

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-3291                                                                                                            |
| <b>State</b>           | PUBLISHED                                                                                                                |
| <b>Assigner</b>        | mitre                                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2012-06-07 20:55:02 UTC                                                                                                  |
| <b>Updated</b>         | 2026-04-29 01:13:23 UTC                                                                                                  |
| <b>Description</b>     | Heap-based buffer overflow in OpenConnect 3.18 allows remote servers to cause a denial of service via a crafted greeting |

## Risk And Classification

**Primary CVSS:** v2.0 7.8 from nvd@nist.gov

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

**Problem Types:** CWE-119 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor    | Product     | Version | Update | Edition | Language |
|-------------|-----------|-------------|---------|--------|---------|----------|
| Application | Infradead | Openconnect | 1.00    | All    | All     | All      |

|             |                           |                             |      |     |     |     |
|-------------|---------------------------|-----------------------------|------|-----|-----|-----|
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 1.10 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 1.20 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 1.30 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 1.40 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.00 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.01 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.10 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.11 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.12 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.20 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.21 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.22 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.23 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.24 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.25 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 2.26 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.00 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.01 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.02 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.11 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.12 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.13 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.14 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.15 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | 3.16 | All | All | All |
| Application | <a href="#">Infradead</a> | <a href="#">Openconnect</a> | All  | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |  |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |  |

| References                                               |                                      |  |  |                                         |      |  |
|----------------------------------------------------------|--------------------------------------|--|--|-----------------------------------------|------|--|
| Reference                                                | Source                               |  |  | Link                                    | Tags |  |
| OpenConnect VPN client.                                  | af854a3a-2127-422b-91ae-364da2661108 |  |  | <a href="#">www.infradead.org</a>       |      |  |
| Debian -- Security Information -- DSA-2495-1 openconnect | af854a3a-2127-422b-91ae-364da2661108 |  |  | <a href="#">www.debian.org</a>          |      |  |
| [SECURITY] Fedora 16 Update: openconnect-3.18-1.fc16     | af854a3a-2127-422b-91ae-364da2661108 |  |  | <a href="#">lists.fedoraproject.org</a> |      |  |
| Repository / Qual Repository                             | af854a3a-2127-422b-91ae-364da2661108 |  |  | <a href="#">qual.susesecurity.org</a>   |      |  |

|                                                                |                                      |                                     |      |
|----------------------------------------------------------------|--------------------------------------|-------------------------------------|------|
| Repository / Oval Repository                                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">oval.cisecurity.org</a> |      |
| openSUSE-SU-2013:1072-1: moderate: update for openconnect      | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">lists.opensuse.org</a>  |      |
| git.infradead.org Git - users/dwmw2/openconnect.git/commitdiff | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">git.infradead.org</a>   |      |
| CVE Program record                                             | CVE.ORG                              | <a href="#">www.cve.org</a>         | cano |
| NVD vulnerability detail                                       | NVD                                  | <a href="#">nvd.nist.gov</a>        | cano |



No vendor comments have been submitted for this CVE.

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