



# CVE-2017-7478

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-7478                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                        |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2017-05-15 18:29:00 UTC                                                                                                    |
| <b>Updated</b>         | 2017-08-16 01:29:00 UTC                                                                                                    |
| <b>Description</b>     | OpenVPN version 2.3.12 and newer is vulnerable to unauthenticated Denial of Service of server via received large control p |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                  | Product                 | Version | Update | Edition | Language |
|-------------|-------------------------|-------------------------|---------|--------|---------|----------|
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.3.12  | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.3.13  | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.3.14  | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | alpha2 | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | beta1  | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | beta2  | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | rc1    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | rc2    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.1   | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.3.12  | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.3.13  | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.3.14  | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | All    | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | alpha2 | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | beta1  | All     | All      |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0   | beta2  | All     | All      |

|             |                         |                         |       |     |     |     |
|-------------|-------------------------|-------------------------|-------|-----|-----|-----|
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0 | rc1 | All | All |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.0 | rc2 | All | All |
| Application | <a href="#">Openvpn</a> | <a href="#">Openvpn</a> | 2.4.1 | All | All | All |

| References                                                                                           |  |  |  |            |                                |  |
|------------------------------------------------------------------------------------------------------|--|--|--|------------|--------------------------------|--|
| Reference                                                                                            |  |  |  | Source     | Link                           |  |
| OpenVPN CVE-2017-7478 Denial of Service Vulnerability                                                |  |  |  | BID        | <a href="#">www.securityfo</a> |  |
| OpenVPN 2.4.0 - Denial of Service - Multiple dos Exploit                                             |  |  |  | EXPLOIT-DB | <a href="#">www.exploit-db</a> |  |
| OpenVPN Packet Processing Flaws Let Remote Users Cause the Target Service to Crash - SecurityTracker |  |  |  | SECTrack   | <a href="#">www.securitytr</a> |  |
| QuarkslabAndCryptographyEngineerAudits – OpenVPN Community                                           |  |  |  | CONFIRM    | <a href="#">community.op</a>   |  |
| CVE Program record                                                                                   |  |  |  | CVE.ORG    | <a href="#">www.cve.org</a>    |  |
| NVD vulnerability detail                                                                             |  |  |  | NVD        | <a href="#">nvd.nist.gov</a>   |  |

No vendor comments have been submitted for this CVE.

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