# CVE-2013-2061

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2013-2061 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2013-11-18 02:55:00 UTC |
| **Updated** | 2020-05-12 14:21:00 UTC |
| **Description** | The openvpn_decrypt function in crypto.c in OpenVPN 2.3.0 and earlier, when running in UDP mode, allows remote attacke |

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Opensuse | Opensuse | 11.4 | All | All | All |
| Operating System | Opensuse | Opensuse | 11.4 | All | All | All |
| Application | Openvpn | Openvpn | 1.2.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.2.1 | All | All | All |
| Application | Openvpn | Openvpn | 1.3.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.3.1 | All | All | All |
| Application | Openvpn | Openvpn | 1.3.2 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.1 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.2 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.3 | All | All | All |
| Application | Openvpn | Openvpn | 1.5.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.6.0 | All | All | All |
| Application | Openvpn | Openvpn | 2.1.0 | All | All | All |
| Application | Openvpn | Openvpn | 2.2.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.2.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.2.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Openvpn | Openvpn | 1.3.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.3.1 | All | All | All |
| Application | Openvpn | Openvpn | 1.3.2 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.1 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.2 | All | All | All |
| Application | Openvpn | Openvpn | 1.4.3 | All | All | All |
| Application | Openvpn | Openvpn | 1.5.0 | All | All | All |
| Application | Openvpn | Openvpn | 1.6.0 | All | All | All |
| Application | Openvpn | Openvpn | 2.1.0 | All | All | All |
| Application | Openvpn | Openvpn | 2.2.0 | All | All | All |
| Application | Openvpn | Openvpn | All | All | All | All |
| Application | Openvpn | Openvpn Access Server | 2.0.0 | All | All | All |
| Application | Openvpn | Openvpn Access Server | 2.0.0 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Bug 960192 – CVE-2013-2061 openvpn: use of non-constant-time memcmp in HMAC comparison in openvpn_decrypt | CONFIRM | bug |
| [SECURITY] Fedora 17 Update: openvpn-2.3.1-2.fc17 | FEDORA | lists |
| SecurityAnnouncement-f375aa67cc – OpenVPN Community | CONFIRM | com |
| Use constant time memcmp when comparing HMACs in openvpn_decrypt. · 11d2134 · OpenVPN/openvpn · GitHub | CONFIRM | gith |
| openSUSE-SU-2013:1649-1: moderate: update for openvpn | SUSE | lists |
| [SECURITY] Fedora 18 Update: openvpn-2.3.1-2.fc18 | FEDORA | lists |
| oss-security - Re: CVE request: OpenVPN use of non-constant-time memcmp in HMAC comparison in openvpn_decrypt | MLIST | www |
| 468756 – (CVE-2013-2061) <net-misc/openvpn-2.3.1: ciphertext injection vulnerability in UDP mode (CVE-2013-2061) | CONFIRM | bug |
| openSUSE-SU-2013:1645-1: moderate: update for openvpn | SUSE | lists |
| Support / Security / Advisories / / MDVSA-2013:167 \| Mandriva | MANDRIVA | www |
| CVE Program record | CVE.ORG | www |
| NVD vulnerability detail | NVD | nvd |

No vendor comments have been submitted for this CVE.

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

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