



# CVE-2013-2061

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

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

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	11.4	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.2.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.2.1	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.3.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.3.1	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.3.2	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.1	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.2	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.3	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.5.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.6.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	2.1.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	2.2.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.2.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.2.1	All	All	All

Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.3.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.3.1	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.3.2	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.1	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.2	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.4.3	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.5.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	1.6.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	2.1.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	2.2.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn</a>	All	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn Access Server</a>	2.0.0	All	All	All
Application	<a href="#">Openvpn</a>	<a href="#">Openvpn Access Server</a>	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	<a href="#">bug</a>
[SECURITY] Fedora 17 Update: openvpn-2.3.1-2.fc17	FEDORA	<a href="#">lists</a>
SecurityAnnouncement-f375aa67cc – OpenVPN Community	CONFIRM	<a href="#">corr</a>
Use constant time memcmp when comparing HMACs in openvpn_decrypt. · 11d2134 · OpenVPN/openvpn · GitHub	CONFIRM	<a href="#">gith</a>
openSUSE-SU-2013:1649-1: moderate: update for openvpn	SUSE	<a href="#">lists</a>
[SECURITY] Fedora 18 Update: openvpn-2.3.1-2.fc18	FEDORA	<a href="#">lists</a>
oss-security - Re: CVE request: OpenVPN use of non-constant-time memcmp in HMAC comparison in openvpn_decrypt	MLIST	<a href="#">ww</a>
468756 – (CVE-2013-2061) <net-misc/openvpn-2.3.1: ciphertext injection vulnerability in UDP mode (CVE-2013-2061)	CONFIRM	<a href="#">bug</a>
openSUSE-SU-2013:1645-1: moderate: update for openvpn	SUSE	<a href="#">lists</a>
Support / Security / Advisories // MDVSA-2013:167   Mandriva	MANDRIVA	<a href="#">ww</a>
CVE Program record	CVE.ORG	<a href="#">ww</a>
NVD vulnerability detail	NVD	<a href="#">nvd</a>

No vendor comments have been submitted for this CVE.

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

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**