



CVE-2012-6128

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

Summary

CVE	CVE-2012-6128
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-24 19:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	Multiple stack-based buffer overflows in http.c in OpenConnect before 4.08 allow remote VPN gateways to cause a denial c

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Infradead	Openconnect	1.00	All	All	All
Application	Infradead	Openconnect	1.10	All	All	All
Application	Infradead	Openconnect	1.20	All	All	All
Application	Infradead	Openconnect	1.30	All	All	All
Application	Infradead	Openconnect	1.40	All	All	All
Application	Infradead	Openconnect	2.00	All	All	All
Application	Infradead	Openconnect	2.01	All	All	All
Application	Infradead	Openconnect	2.10	All	All	All
Application	Infradead	Openconnect	2.11	All	All	All
Application	Infradead	Openconnect	2.12	All	All	All
Application	Infradead	Openconnect	2.20	All	All	All
Application	Infradead	Openconnect	2.21	All	All	All
Application	Infradead	Openconnect	2.22	All	All	All
Application	Infradead	Openconnect	2.23	All	All	All
Application	Infradead	Openconnect	2.24	All	All	All
Application	Infradead	Openconnect	2.25	All	All	All
Application	Infradead	Openconnect	2.26	All	All	All

Application	Infradead	Openconnect	3.00	All	All	All
Application	Infradead	Openconnect	3.01	All	All	All
Application	Infradead	Openconnect	3.02	All	All	All
Application	Infradead	Openconnect	3.11	All	All	All
Application	Infradead	Openconnect	3.12	All	All	All
Application	Infradead	Openconnect	3.13	All	All	All
Application	Infradead	Openconnect	3.14	All	All	All
Application	Infradead	Openconnect	3.15	All	All	All
Application	Infradead	Openconnect	3.16	All	All	All
Application	Infradead	Openconnect	3.17	All	All	All
Application	Infradead	Openconnect	3.18	All	All	All
Application	Infradead	Openconnect	3.19	All	All	All
Application	Infradead	Openconnect	3.20	All	All	All
Application	Infradead	Openconnect	3.99	All	All	All
Application	Infradead	Openconnect	4.00	All	All	All
Application	Infradead	Openconnect	4.01	All	All	All
Application	Infradead	Openconnect	4.02	All	All	All
Application	Infradead	Openconnect	4.03	All	All	All
Application	Infradead	Openconnect	4.04	All	All	All
Application	Infradead	Openconnect	4.05	All	All	All
Application	Infradead	Openconnect	4.06	All	All	All
Application	Infradead	Openconnect	1.00	All	All	All
Application	Infradead	Openconnect	1.10	All	All	All
Application	Infradead	Openconnect	1.20	All	All	All
Application	Infradead	Openconnect	1.30	All	All	All
Application	Infradead	Openconnect	1.40	All	All	All
Application	Infradead	Openconnect	2.00	All	All	All
Application	Infradead	Openconnect	2.01	All	All	All
Application	Infradead	Openconnect	2.10	All	All	All
Application	Infradead	Openconnect	2.11	All	All	All
Application	Infradead	Openconnect	2.12	All	All	All
Application	Infradead	Openconnect	2.20	All	All	All
Application	Infradead	Openconnect	2.21	All	All	All
Application	Infradead	Openconnect	2.22	All	All	All
Application	Infradead	Openconnect	2.23	All	All	All

Application	Infradead	Openconnect	2.24	All	All	All
Application	Infradead	Openconnect	2.25	All	All	All
Application	Infradead	Openconnect	2.26	All	All	All
Application	Infradead	Openconnect	3.00	All	All	All
Application	Infradead	Openconnect	3.01	All	All	All
Application	Infradead	Openconnect	3.02	All	All	All
Application	Infradead	Openconnect	3.11	All	All	All
Application	Infradead	Openconnect	3.12	All	All	All
Application	Infradead	Openconnect	3.13	All	All	All
Application	Infradead	Openconnect	3.14	All	All	All
Application	Infradead	Openconnect	3.15	All	All	All
Application	Infradead	Openconnect	3.16	All	All	All
Application	Infradead	Openconnect	3.17	All	All	All
Application	Infradead	Openconnect	3.18	All	All	All
Application	Infradead	Openconnect	3.19	All	All	All
Application	Infradead	Openconnect	3.20	All	All	All
Application	Infradead	Openconnect	3.99	All	All	All
Application	Infradead	Openconnect	4.00	All	All	All
Application	Infradead	Openconnect	4.01	All	All	All
Application	Infradead	Openconnect	4.02	All	All	All
Application	Infradead	Openconnect	4.03	All	All	All
Application	Infradead	Openconnect	4.04	All	All	All
Application	Infradead	Openconnect	4.05	All	All	All
Application	Infradead	Openconnect	4.06	All	All	All
Application	Infradead	Openconnect	All	All	All	All

References						
Reference			Source	Link	Tags	
Support / Security / Advisories / / MDVSA-2013:108 Mandriva			MANDRIVA	www.mandriva.com		
IBM X-Force Exchange			XF	exchange.xforce.ibmcloud.com		
Debian -- Security Information -- DSA-2623-1 openconnect			DEBIAN	www.debian.org	Vendor Advisory	
OpenConnect VPN Gateway Stack Based Buffer Overflow Vulnerability			BID	www.securityfocus.com	Vendor Advisory	
Support/Advisories/MGASA-2013-0060 - Mageia wiki			CONFIRM	wiki.mageia.org		
openSUSE-SU-2013:0979-1: moderate: update for openconnect			SUSE	lists.opensuse.org		
OpenConnect VPN client.			CONFIRM	www.infradead.org		
git.infradead.org Git - users/dwmw2/openconnect.git/commitdiff			CONFIRM	git.infradead.org	Vendor Advisory	

oss-security - Re: CVE request: openconnect buffer overflow	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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