



CVE-2013-2070

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

Summary

CVE	CVE-2013-2070
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-20 03:37:00 UTC
Updated	2021-11-10 15:59:00 UTC
Description	http/modules/nginx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	F5	Nginx	All	All	All	All
Application	F5	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Nginx	Nginx	All	All	All	All

References

Reference	Source	Link
Nginx CVE-2013-2070 Remote Security Vulnerability	BID	www.securityfocus.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
oss-sec: Re: nginx security advisory (CVE-2013-2028)	MLIST	seclists.org
[SECURITY] Fedora 18 Update: nginx-1.2.9-1.fc18	FEDORA	lists.fedoraproject.org
nginx.org/download/patch.2013.proxy.txt	MISC	nginx.org
Debian -- Security Information -- DSA-2721-1 nginx	DEBIAN	www.debian.org

About Secunia Research Flexera	SECUNIA	secunia.com
[nginx-announce] nginx security advisory (CVE-2013-2070)	MLIST	mailman.nginx.org
oss-security - nginx security advisory (CVE-2013-2070)	MLIST	www.openwall.com
Bug 962525 – CVE-2013-2070 nginx: denial of service or memory disclosure when using proxy_pass	MISC	bugzilla.redhat.com
Gentoo Linux Documentation -- nginx: Multiple vulnerabilities	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://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