



CVE-2013-1049

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-1049
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-03-14 03:13:00 UTC
Updated	2013-03-19 04:00:00 UTC
Description	Buffer overflow in the RFC1413 (ident) client in cfingerd 1.4.3-3 allows remote IDENT servers to cause a denial of service (

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Debian	Cfingerd	1.4.3-3	All	All	All
Application	Debian	Cfingerd	1.4.3-3	All	All	All

References

Reference	Source	Link
Bug #1104425 "SECURITY: remotely-exploitable buffer overflow in ...": Bugs : "cfingerd" package : Ubuntu	MISC	bugs.launchpad.net
90747	OSVDB	osvdb.org
Debian -- Security Information -- DSA-2635-1 cfingerd	DEBIAN	www.debian.org
#700098 - cfingerd: CVE-2013-1049 remote buffer overflow - Debian Bug report logs	MISC	bugs.debian.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](#) 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](#) 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](#)