CVE-2015-5400

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-5400
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-28 20:59:00 UTC
Updated	2017-09-22 01:29:00 UTC
Description	Squid before 3.5.6 does not properly handle CONNECT method peer responses when configured with cache_peer, which a

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Squid-cache	Squid	All	All	All	All

References

Reference	Source	L
www.squid-cache.org/Advisories/SQUID-2015_2.txt	CONFIRM	v
[security-announce] SUSE-SU-2016:2089-1: important: Security update for	SUSE	li
oss-security - Squid HTTP proxy CVE request	MLIST	v
oss-security - Re: Squid HTTP proxy CVE request	MLIST	v
oss-security - Re: Squid HTTP proxy CVE request	MLIST	v
Debian -- Security Information -- DSA-3327-1 squid3	DEBIAN	v
Squid CONNECT Method Peer Response Processing Flaw Lets Remote Users Bypass Security Controls - SecurityTracker	SECTRACK	v

[SECURITY] Fedora 22 Update: libecap-1.0.0-1.fc22	FEDORA	li
www.squid-cache.org/Versions/v3/3.5/changesets/squid-3.5-13856.patch	CONFIRM	v
[security-announce] SUSE-SU-2016:1996-1: important: Security update for	SUSE	li
oss-security - Re: Squid HTTP proxy CVE request	MLIST	v
www.squid-cache.org/Versions/v3/3.1/changesets/squid-3.1-10494.patch	CONFIRM	v
www.squid-cache.org/Versions/v3/3.4/changesets/squid-3.4-13225.patch	CONFIRM	v
Squid Denial of Service and Security Bypass Vulnerabilities	BID	v
openSUSE-SU-2016:2081-1: moderate: Security update for squid	SUSE	li
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

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 registred 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.

Free CVE JSON API cve.report/api

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