



CVE-2016-3947

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

Summary

CVE	CVE-2016-3947
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-07 18:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Heap-based buffer overflow in the Icmp6::Recv function in icmp/lcmp6.cc in the pinger utility in Squid before 3.5.16 and 4.x

Risk And Classification

Primary CVSS: v3.0 8.2 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Problem Types: CWE-119 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.2	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Application	Squid-cache	Squid	4.0.1	All	All	All
Application	Squid-cache	Squid	4.0.2	All	All	All
Application	Squid-cache	Squid	4.0.3	All	All	All
Application	Squid-cache	Squid	4.0.4	All	All	All
Application	Squid-cache	Squid	4.0.5	All	All	All
Application	Squid-cache	Squid	4.0.6	All	All	All
Application	Squid-cache	Squid	4.0.7	All	All	All
Application	Squid-cache	Squid	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
www.squid-cache.org/Advisories/SQUID-2016_3.txt
openSUSE-SU-2016:2081-1: moderate: Security update for squid
Squid: Multiple vulnerabilities (GLSA 201607-01) — Gentoo security
www.squid-cache.org/Versions/v3/3.3/changesets/squid-3.3-12694.patch
www.squid-cache.org/Versions/v3/3.2/changesets/squid-3.2-11839.patch
[security-announce] SUSE-SU-2016:1996-1: important: Security update for
Squid Bug in ICMPv6 Pinger Lets Remote Users Deny Service and Local Users Obtain Potentially Sensitive Heap Memory Contents - Security
USN-2995-1: Squid vulnerabilities Ubuntu
www.squid-cache.org/Versions/v3/3.5/changesets/squid-3.5-14015.patch
[security-announce] SUSE-SU-2016:2089-1: important: Security update for
www.squid-cache.org/Versions/v3/3.4/changesets/squid-3.4-13232.patch
www.squid-cache.org/Versions/v3/3.1/changesets/squid-3.1-10495.patch
CVE Program record
NVD vulnerability detail

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