CVE-2005-0096

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

Summary

CVE	CVE-2005-0096
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-25 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Memory leak in the NTLM fakeauth_auth helper for Squid 2.5.STABLE7 and earlier allows remote attackers to cause a den

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squid	Squid	2.0_patch2	All	All	All

Application	Squid	Squid	2.1_patch2	All	All	All
Application	Squid	Squid	2.3_.stable4	All	All	All
Application	Squid	Squid	2.3_.stable5	All	All	All
Application	Squid	Squid	2.3_stable5	All	All	All
Application	Squid	Squid	2.4	All	All	All
Application	Squid	Squid	2.4_.stable2	All	All	All
Application	Squid	Squid	2.4_.stable6	All	All	All
Application	Squid	Squid	2.4_.stable7	All	All	All
Application	Squid	Squid	2.4_stable7	All	All	All
Application	Squid	Squid	2.5.6	All	All	All
Application	Squid	Squid	2.5.stable1	All	All	All
Application	Squid	Squid	2.5.stable2	All	All	All
Application	Squid	Squid	2.5.stable3	All	All	All
Application	Squid	Squid	2.5.stable4	All	All	All
Application	Squid	Squid	2.5.stable5	All	All	All
Application	Squid	Squid	2.5.stable6	All	All	All
Application	Squid	Squid	2.5.stable7	All	All	All
Application	Squid	Squid	2.5_.stable1	All	All	All
Application	Squid	Squid	2.5_.stable3	All	All	All
Application	Squid	Squid	2.5_.stable4	All	All	All
Application	Squid	Squid	2.5_.stable5	All	All	All
Application	Squid	Squid	2.5_.stable6	All	All	All
Application	Squid	Squid	2.5_stable3	All	All	All
Application	Squid	Squid	2.5_stable4	All	All	All
Application	Squid	Squid	2.5_stable9	All	All	All
Application	Squid	Squid	2.6.stable1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Security Announcement	af854a3a-2127-422b-91ae-364da26
404 Not Found	af854a3a-2127-422b-91ae-364da26
Gentoo Linux Documentation -- Squid: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da26
Home - Conectiva	af854a3a-2127-422b-91ae-364da26

Home - Conectiva	af854a3a-2127-422b-91ae-364da26
www.trustix.org/errata/2005/0003	af854a3a-2127-422b-91ae-364da26
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da26
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da26
SecurityTracker.com Archives - Squid NTLM fakeauth_auth Helper Can Be Crashed By Remote Users	af854a3a-2127-422b-91ae-364da26
Squid-2.5 Patches	af854a3a-2127-422b-91ae-364da26
Squid Proxy NTLM Fakeauth_Auth Memory Leak Remote Denial Of Service Vulnerability	af854a3a-2127-422b-91ae-364da26
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da26
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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**