



CVE-2005-0175

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

Summary

CVE	CVE-2005-0175
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-02-07 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Squid 2.5 up to 2.5.STABLE7 allows remote attackers to poison the cache via an HTTP response splitting attack.

Risk And Classification

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

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

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

References						
Reference			Source		Link	
[SECURITY] Fedora Core 3 Update: squid-2.5.STABLE9-1.FC3.6			af854a3a-2127-422b-91ae-364da2661108		www.redhat.com	
Security Announcement			af854a3a-2127-422b-91ae-364da2661108		www.novell.com	
404 Not Found			af854a3a-2127-422b-91ae-364da2661108		fedoranews.org	
Advisories - Mandriva			af854a3a-2127-422b-91ae-364da2661108		www.mandriva.c	
www.squid-cache.org/Advisories/SQUID-2005_5.txt			af854a3a-2127-422b-91ae-364da2661108		www.squid-cache	
Repository / Oval Repository			af854a3a-2127-422b-91ae-364da2661108		oval.cisecurity.or	
US-CERT Vulnerability Note VU#625878			af854a3a-2127-422b-91ae-364da2661108		www.kb.cert.org	
rhn.redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		www.redhat.com	
Squid-2.5 Patches			af854a3a-2127-422b-91ae-364da2661108		www.squid-cache	
rhn.redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		www.redhat.com	
Home - Conectiva			af854a3a-2127-422b-91ae-364da2661108		distro.conectiva.c	
Debian -- Security Information -- DSA-667-1 squid			af854a3a-2127-422b-91ae-364da2661108		www.debian.org	
Squid Proxy Malformed HTTP Header Parsing Cache Poisoning Vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.securityfocu	
'[USN-77-1] Squid vulnerabilities' - MARC			af854a3a-2127-422b-91ae-364da2661108		marc.info	
CVE Program record			CVE.ORG		www.cve.org	

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)