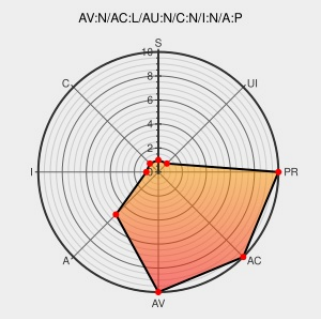
CVE-2004-2654

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2654

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Squid from Squid contain the following vulnerability:

The clientAbortBody function in client_side.c in Squid Web Proxy Cache before 2.6 STABLE6 allows remote attackers to cause a denial of service (segmentation fault) via unspecified vectors that trigger a null dereference. NOTE: in a followup advisory, a researcher claimed that the issue was a buffer overflow that was not fixed in STABLE6. However, the vendor's bug report clearly shows that the researcher later retracted this claim, because the tested product was actually STABLE5.

CVE-2004-2654 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
404 Not Found	www.squid-cache.org, text/html, Inactive Link, Not Archived	MISC www.squid-cache.org/bugs/show_bug.cgi?id=972
[VIM] old Squid clientAbortBody issue - NOT an overflow?	www.attrition.org, text/html	VIM 20060223 old Squid clientAbortBody issue - NOT an overflow?
404 - Страница не найдена	web.archive.org, text/html, Inactive Link, Not Archived	MISC www.securitylab.ru/47881.html
Secunia - Advisories - Squid "clientAbortBody()" and PUT/POST Denial of Service Vulnerabilities	Vendor Advisory, web.archive.org	SECUNIA 12508

	text/html	
Secunia - Advisories - Fedora update for squid	Patch Vendor Advisory web.archive.org text/html	SECUNIA 12754
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 9801
SecurityTracker.com Archives - Squid Null Pointer Dereference in clientAbortBody() Lets Remote Users Crash the Proxy	securitytracker.com text/html	SECTRACK 1011214

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squid	Squid	2.5_stable5	All	All	All
Application	Squid	Squid	2.5_stable5	All	All	All

cpe:2.3:a:squid:squid:2.5_stable5:*:*:*:*:*:*:*:

cpe:2.3:a:squid:squid:2.5_stable5:*:*:*:*:*:*:*:

← Previous ID

Next ID→