



CVE-2009-2855

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-2855
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-18 21:00:00 UTC
Updated	2023-11-07 02:04:00 UTC
Description	The strListGetItem function in src/HTTPHeaderTools.c in Squid 2.7 allows remote attackers to cause a denial of service via a

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Squid-cache	Squid	2.7	All	All	All
Application	Squid-cache	Squid	2.7	stable3	All	All
Application	Squid-cache	Squid	2.7	stable4	All	All
Application	Squid-cache	Squid	2.7	All	All	All
Application	Squid-cache	Squid	2.7	stable3	All	All
Application	Squid-cache	Squid	2.7	stable4	All	All

References

Reference	Source	Link
Repository / Oval Repository	OVAL	oval
oss-security - Re: squid DoS in external auth header parser	MLIST	www
Squid Web Proxy Cache Authentication Header Parsing Remote Denial of Service Vulnerability	BID	www
oss-security - Re: squid DoS in external auth header parser	MLIST	www
Error		bugs
404 Not Found	MISC	www
oss-security - squid DoS in external auth header parser	MLIST	www
bugs.debian.org/cgi-bin/bugreport.cgi	MISC	bugs

#534982 - squid - DoS in external auth header parser - Debian Bug report logs	CONFIRM	bug
404 Not Found	CONFIRM	ww
IBM X-Force Exchange	XF	ex
SecurityTracker.com Archives - Squid Infinite Loop in strListItem() Lets Remote Users Deny Service	SECTrack	ww
Bug 518182 – CVE-2009-2855 squid: DoS (100% CPU use) while processing certain external ACL helper HTTP headers	CONFIRM	bu
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-03-31	Tomas Hoger	This issue did not affect the versions of the squid packages, as shipped with Red Hat Enterprise



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](#)