



# CVE-2009-0801

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

## Summary

<b>CVE</b>	CVE-2009-0801
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-03-04 16:30:00 UTC
<b>Updated</b>	2009-06-18 04:00:00 UTC
<b>Description</b>	Squid, when transparent interception mode is enabled, uses the HTTP Host header to determine the remote endpoint, which

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	2.7	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	2.7.stable5	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	2.7.stable6	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_pre1	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_pre2	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_pre3	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable1	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable12	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable13	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable2	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable3	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable4	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable5	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable6	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable7	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	2.7	All	All	All

Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	2.7.stable5	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	2.7.stable6	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_pre1	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_pre2	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_pre3	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable1	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable12	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable13	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable2	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable3	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable4	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable5	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable6	All	All	All
Application	<a href="#">Squid</a>	<a href="#">Squid Web Proxy Cache</a>	3.0_stable7	All	All	All

## References

Reference	Source	Link	Tags
Multiple HTTP Proxy HTTP Host Header Incorrect Relay Behavior Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
US-CERT Vulnerability Note VU#435052	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-03-09	Joshua Bressers	Red Hat is aware of this issue and is tracking it via the following bug: <a href="https://bugzilla.redhat.com/show_bug.cgi?id=435052">https://bugzilla.redhat.com/show_bug.cgi?id=435052</a>

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)