



CVE-2008-7160

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

Summary

CVE	CVE-2008-7160
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-10 21:30:00 UTC
Updated	2012-10-23 03:01:00 UTC
Description	The silc_http_server_parse function in lib/silchttp/silchttpserver.c in the internal HTTP server in silcd in Secure Internet Live

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Silcnet	Silc Toolkit	1.1	All	All	All
Application	Silcnet	Silc Toolkit	1.1.1	All	All	All
Application	Silcnet	Silc Toolkit	1.1.2	All	All	All
Application	Silcnet	Silc Toolkit	1.1.3	All	All	All
Application	Silcnet	Silc Toolkit	1.1.4	All	All	All
Application	Silcnet	Silc Toolkit	1.1.5	All	All	All
Application	Silcnet	Silc Toolkit	1.1.6	All	All	All
Application	Silcnet	Silc Toolkit	1.1	All	All	All
Application	Silcnet	Silc Toolkit	1.1.1	All	All	All
Application	Silcnet	Silc Toolkit	1.1.2	All	All	All
Application	Silcnet	Silc Toolkit	1.1.3	All	All	All
Application	Silcnet	Silc Toolkit	1.1.4	All	All	All
Application	Silcnet	Silc Toolkit	1.1.5	All	All	All
Application	Silcnet	Silc Toolkit	1.1.6	All	All	All
Application	Silcnet	Silc Toolkit	All	All	All	All

References

Reference	Source	Link
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:016	SUSE	lists.opensuse.org
Security Advisory SA36625 - SILC Toolkit / SILC Server Incorrect Format Specifier Memory Corruption - Secunia	SECUNIA	secunia.com
Support / Security / Advisories / / MDVSA-2009:234 Mandriva	MANDRIVA	www.mandriva.com
404 Not Found	CONFIRM	silcnet.org
SILC Toolkit HTTP Server Format String Vulnerability	BID	www.securityfocus.com
Debian -- Security Information -- DSA-1879-1 silc-client/silc-toolkit	DEBIAN	www.debian.org
Debian update for silc-client and silc-toolkit - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
SILC Secure Internet Live Conferencing	CONFIRM	silcnet.org
oss-security - CVE id request: silc-toolkit	MLIST	www.openwall.com
oss-security - Re: CVE id request: silc-toolkit	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2009-09-11	Tomas Hoger	Not vulnerable. This issue did not affect the versions of libsilc as shipped with Red Hat Enterprise Linux 5.

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](#)