



CVE-2008-1429

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

Summary

CVE	CVE-2008-1429
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-20 18:44:00 UTC
Updated	2017-08-08 01:30:00 UTC
Description	Secure Internet Live Conferencing (SILC) Server before 1.1.1 allows remote attackers to cause a denial of service (daemor

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Silc	Silc-server	All	All	All	All

References

Reference	Source
Secure Internet Live Conferencing (SILC) Can Be Crashed By Remote Users With a NEW_CLIENT Packet - SecurityTracker	SECTRAK
SILC Server "NEW_CLIENT" Packet Denial of Service - Advisories - Secunia	SECUNIA
SILC: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SILC Server 'NEW_CLIENT' Remote Denial of Service Vulnerability	BID
IBM X-Force Exchange	XF
Gentoo update for silc - Advisories - Secunia	SECUNIA
404 Not Found	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)