



CVE-2007-5690

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

Summary

CVE	CVE-2007-5690
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-29 19:46:00 UTC
Updated	2023-11-07 02:01:00 UTC
Description	** DISPUTED ** Buffer overflow in sethdlc.c in the Asterisk Zaptel 1.4.5.1 might allow local users to gain privileges via a lon

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asterisk	Zaptel	1.4.5.1	All	All	All
Application	Asterisk	Zaptel	1.4.5.1	All	All	All

References

Reference	Sou
SecurityFocus	BUG
eleytt.com	MIS
IBM X-Force Exchange	XF
SecurityFocus	BUG
AST-2007-024	MIS
CXSecurity - IDS	SRE
Zaptel SethDLC.C Local Buffer Overflow Vulnerability	BID
[Vendor Disputes Security Impact] Zaptel Buffer Overflow in 'sethdlc.c' May Let Local Users Gain Elevated Privileges - SecurityTracker	SEC
CVE Program record	CVE
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](#)