



CVE-2000-0964

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

Summary

CVE	CVE-2000-0964
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-12-19 05:00:00 UTC
Updated	2017-10-10 01:29:00 UTC
Description	Buffer overflow in the web administration service for the HiNet LP5100 IP-phone allows remote attackers to cause a denial of service (CPU usage) by sending a crafted SIP message. The vulnerability exists in the SIP message processing function in the web administration service. The vulnerability is caused by a buffer overflow in the SIP message processing function. The vulnerability is caused by a buffer overflow in the SIP message processing function. The vulnerability is caused by a buffer overflow in the SIP message processing function.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Hinet Lp	5100.0	All	All	All
Hardware	Siemens	Hinet Lp	5100.0	All	All	All

References

Reference	Source	Link	Tags
Siemens HiNet LP5100 IP-phone Buffer Overflow DoS Vulnerability	BID	www.securityfocus.com	Vendor Advisory
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
20000928 Another thingy.	BUGTRAQ	archives.neohapsis.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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