



CVE-2007-2270

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

Summary

CVE	CVE-2007-2270
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-25 20:19:00 UTC
Updated	2017-10-11 01:32:00 UTC
Description	The Linksys SPA941 VoIP Phone allows remote attackers to cause a denial of service (device reboot) via a 0377 (0xff) cha

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Linksys	Spa941	All	All	All	All
Hardware	Linksys	Spa941	All	All	All	All

References

Reference	Source	Link
Linksys SPA941 \377 Character Denial of Service Vulnerability	BID	www.securityfocu
Linksys SPA941 Phone Can Be Crashed By Remote Users - SecurityTracker	SECTrack	www.securitytrac
Linksys SPA941 SIP Message Denial of Service - Advisories - Secunia	SECUNIA	secunia.com
Linksys SPA941 377 character Remote Denial of Service Exploit	EXPLOIT-DB	www.exploit-db.c
[Full-disclosure] ZDI-07-022: CA BrightStor ArcServe Media Server Multiple Buffer Overflow Vulnerabilities	FULLDISC	lists.grok.org.uk
Linksys SPA941 (remote reboot) Remote Denial of Service Exploit	EXPLOIT-DB	www.exploit-db.c
IBM X-Force Exchange	XF	exchange.xforce.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)