



CVE-2021-26728

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

Summary

CVE	CVE-2021-26728
State	PUBLIC
Assigner	prodsec@nozominetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-24 14:15:00 UTC
Updated	2022-12-03 15:08:00 UTC
Description	Command injection and stack-based buffer overflow vulnerabilities in the KillDupUsr_func function of spx_restservice allow

Risk And Classification

Problem Types: CWE-77 | CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Lannerinc	lac-ast2500a	-	All	All	All
Operating System	Lannerinc	lac-ast2500a Firmware	1.10.0	All	All	All

References

Reference	Source	Link	Tags
cvelist/CVE-2021-26728.json at master · CVEProject/cvelist · GitHub	MISC	github.com	Third Party Advisory
Vulnerabilities in BMC Firmware Affect OT/IoT Device Security – Part 1	MISC	www.nozominetworks.com	
www.nozominetworks.com/labs/vulnerability-advisories/cve-2021-26728	MISC	www.nozominetworks.com	
Error 404	MISC	www.nozominetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Andrea Palanca of Nozomi Networks found this bug during a security research activity.

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](#)