CVE-2023-33621

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-33621
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-13 16:15:00 UTC
Updated	2023-06-23 19:18:00 UTC
Description	GL.iNET GL-AR750S-Ext firmware v3.215 inserts the admin authentication token into a GET request when the OpenVPN S

Risk And Classification

Problem Types: CWE-294

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Gl-inet	Gl-ar750s	-	All	All	All
Operating System	Gl-inet	Gl-ar750s Firmware	3.215	All	All	All

References

Reference	Source	Link	Tags
gl-ar750s-ext.com	MISC	gl-ar750s-ext.com	
glinet.com	MISC	glinet.com	
CVE-2023-33621: GL.iNET Auth Token in GET Query String - Justin Applegate	MISC	justinapplegate.me	
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report