CVE-2020-5782

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

Summary

CVE	CVE-2020-5782
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-23 16:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	In IgniteNet HeliOS GLinq v2.2.1 r2961, if a user logs in and sets the 'wan_type' parameter, the wan interface for the device

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ignitenet	Helios Glinq	2.2.1	r2961	All	All
Application	Ignitenet	Helios Glinq	2.2.1	r2961	All	All

References

Reference	Source	Link	Tags
IgniteNet HeliOS GLinq v2.2.1 r2961 Multiple Vulnerabilities - Research Advisory | Tenable®	MISC	www.tenable.com	Exploit, Third
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

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**