



CVE-2020-5783

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

Summary

CVE	CVE-2020-5783
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-23 16:15:00 UTC
Updated	2020-09-29 14:15:00 UTC
Description	In IgniteNet HeliOS GLinq v2.2.1 r2961, the login functionality does not contain any CSRF protection mechanisms.

Risk And Classification

Problem Types: CWE-352

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, Thirc
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.

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