CVE-2020-19202

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

Summary

CVE	CVE-2020-19202
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-17 16:15:00 UTC
Updated	2021-06-22 15:27:00 UTC
Description	An authenticated Stored XSS (Cross-site Scripting) exists in the "captive.cgi" Captive Portal via the "Title of Login Page" tex

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ipfire	Ipfire	2.21	core_update130	All	All

References

Reference	Source	Link	Tags
blog.ipfire.org - IPFire 2.23 - Core Update 132 released	MISC	blog.ipfire.org	
Authenicated Stored XSS in IPFire 2.21 · GitHub	MISC	gist.github.com	
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**