



CVE-2020-19204

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

Summary

CVE	CVE-2020-19204
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-12 16:15:00 UTC
Updated	2022-04-29 17:15:00 UTC
Description	An authenticated Stored Cross-Site Scripting (XSS) vulnerability exists in Lightning Wire Labs IPFire 2.21 (x86_64) - Core

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
Authenticated Stored XSS in IPFire 2.21 · GitHub	MISC	gist.github.com	
blog.ipfire.org - IPFire 2.23 - Core Update 133 has been released	MISC	blog.ipfire.org	
Lightning Wire Labs	MISC	www.lightningwirelabs.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.

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