CVE-2020-29596

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

Summary

CVE	CVE-2020-29596
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-21 22:15:00 UTC
Updated	2020-12-23 18:13:00 UTC
Description	MiniWeb HTTP server 0.8.19 allows remote attackers to cause a denial of service (daemon crash) via a long name for the f

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniweb Http Server Project	Miniweb Http Server	0.8.19	All	All	All
Application	Miniweb Http Server Project	Miniweb Http Server	0.8.19	All	All	All

References

Reference	Source	Link	Tags
MiniWeb HTTP Server 0-day Vulnerability (CVE-2020-29596)	MISC	securityforeveryone.com	Third Party Advis
MiniWeb HTTP server - Browse /miniweb/0.8 at SourceForge.net	MISC	sourceforge.net	Product, Third Pa
MiniWeb HTTP Server 0.8.19 - Buffer Overflow (PoC) - Multiple webapps Exploit	MISC	www.exploit-db.com	Exploit, Third Par
MiniWeb HTTP Server 0.8.19 Buffer Overflow ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Par
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

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