



CVE-2020-21588

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

Summary

CVE	CVE-2020-21588
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-02 20:15:00 UTC
Updated	2021-04-08 15:46:00 UTC
Description	Buffer overflow in Core FTP LE v2.2 allows local attackers to cause a denial or service (crash) via a long string in the Setup

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coreftp	Core Ftp	2.2	All	All	All

References

Reference	Source	Link	Tags
Core FTP Local DOS Vulnerability · Issue #1 · pwnninja/CoreFTP · GitHub	MISC	github.com	
Core FTP Local DOS Vulnerability · Issue #1 · pwnninja/CoreFTP · GitHub	MISC	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.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)