



CVE-2018-20658

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-20658
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-02 15:29:00 UTC
Updated	2019-01-31 17:20:00 UTC
Description	The server in Core FTP 2.0 build 653 on 32-bit platforms allows remote attackers to cause a denial of service (daemon crash) via a crafted request.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coreftp	Core Ftp	2.0	All	All	All
Application	Coreftp	Core Ftp	2.0	All	All	All

References

Reference	Source	Link	Tags
Core FTP 2.0 - 'XRMD' Denial of Service (PoC) - Windows dos Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, Third Party Advisory,
Server v2 build 725 - Core FTP	MISC	coreftp.com	Third Party Advisory
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.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

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