



CVE-2020-5194

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

Summary

CVE	CVE-2020-5194
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-14 14:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	The zip API endpoint in Cerberus FTP Server 8 allows an authenticated attacker without zip permission to use the zip funct

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cerberusftp	Ftp Server	8.0	All	All	All
Application	Cerberusftp	Ftp Server	8.0	All	All	All

References

Reference	Source	Link	Tags
Announcements – Cerberus Support	MISC	support.cerberusftp.com	Vend
Cerberus FTP Vulnerabilities – CVE-2020-5194, CVE-2020-5195, CVE-2020-5196 doyle.net	MISC	www.doyle.net	Expl
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report