



CVE-2021-40524

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

Summary

CVE	CVE-2021-40524
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-05 19:15:00 UTC
Updated	2021-11-26 19:49:00 UTC
Description	In Pure-FTPd before 1.0.50, an incorrect max_filesize quota mechanism in the server allows attackers to upload files of un

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pureftpd	Pure-ftp	All	All	All	All
Application	Pureftpd	Pure-ftp	1.0.49	All	All	All

References

Reference	Source	Link	Tags
Initialize the max upload file size when quotas are enabled · jedisct1/pure-ftp@37ad222 · GitHub	CONFIRM	github.com	
fix the maxfile_size checking bug by DroidTest · Pull Request #158 · jedisct1/pure-ftp · GitHub	MISC	github.com	
Comparing 1.0.49...1.0.50 · jedisct1/pure-ftp · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184881 Debian Security Update for pure-ftp (CVE-2021-40524)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)