



CVE-2020-27955

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

Summary

CVE	CVE-2020-27955
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-05 15:15:00 UTC
Updated	2021-12-16 20:35:00 UTC
Description	Git LFS 2.12.0 allows Remote Code Execution.

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Git Large File Storage Project	Git Large File Storage	2.12.0	All	All	All
Application	Git Large File Storage Project	Git Large File Storage	2.12.0	All	All	All

References

Reference	Source	Link
Git git-lfs Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity
Releases · git-lfs/git-lfs · GitHub	MISC	github.com
Git-LFS-RCE-Exploit-CVE-2020-27955-for-safety	MISC	legalhackers.com
Legal/ethical hacking. Information security.	MISC	legalhackers.com
ExploitBox.io - A playground & labs For Hackers, 0day Bug Hunters, Pentesters, Security Researchers	MISC	exploitbox.io
Full Disclosure: Git LFS (git-lfs) - Remote Code Execution (RCE) exploit CVE-2020-27955 - Clone to Pwn	FULLDISC	seclists.org
git-lfs Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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