



CVE-2021-40323

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

Summary

CVE	CVE-2021-40323
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-04 06:15:00 UTC
Updated	2021-10-12 20:25:00 UTC
Description	Cobbler before 3.3.0 allows log poisoning, and resultant Remote Code Execution, via an XMLRPC method that logs to the I

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cobbler Project	Cobbler	All	All	All	All

References

Reference	Source	Link	Tags
Release Cobbler V3.3.0 · cobbler/cobbler · GitHub	MISC	github.com	
Merge pull request #2794 from cobbler/fix/file-rce · cobbler/cobbler@d8f60bb · 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.

Legacy QID Mappings

199906 Ubuntu Security Notification for Cobbler Vulnerabilities (USN-6475-1)
281953 Fedora Security Update for cobbler (FEDORA-2021-4def184821)
281954 Fedora Security Update for cobbler (FEDORA-2021-5f1e30aa56)
730828 Cobbler Remote Code Execution(RCE) Vulnerability

© [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](#)