



CVE-2018-1000225

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

Summary

CVE	CVE-2018-1000225
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-20 20:29:00 UTC
Updated	2018-10-19 17:33:00 UTC
Description	Cobbler version Verified as present in Cobbler versions 2.6.11+, but code inspection suggests at least 2.0.0+ or possibly ev

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Persistent XSS vulnerability in cobbler-web [CVE-2018-1000225] · Issue #1917 · cobbler/cobbler · GitHub	CONFIRM	github.com
Privilege Escalation Exploits in Cobbler's API	MISC	movermeyer.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199906](#) Ubuntu Security Notification for Cobbler Vulnerabilities (USN-6475-1)

[750439](#) OpenSUSE Security Update for cobbler (openSUSE-SU-2021:0046-1)

© [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](#)