An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2411220144

NCSC Advisory

A Critical Vulnerability Exists In: Cobbler Server

(CVSSv3: 9.8)

22nd, November 2024

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Description

CVE ID: CVE-2024-47533

Published: 2024-11-18

Vendor: N/A

Product: Cobbler Server

CVSS3.0 Score[1]: 9.8

Products affected

Product	Versions
Cobbler Server	3.0.0 < 3.2.3
Cobbler Server	3.3.0 < 3.3.7

Impact

Cobbler, a Linux installation server that allows for rapid setup of network installation environments, has an improper authentication vulnerability starting in version 3.0.0 and versions prior to 3.2.3 and 3.3.7.

`utils.get_shared_secret()` always returns `-1`, which allows anyone to connect to cobbler XML-RPC as user `"` password `-1` and make any changes. This gives anyone with network access to a Cobbler server full control of the server. This issue is fixed in versions **3.2.3** and **3.3.7**.

Common Weakness Enumeration (CWE)[2]: CWE-287: Improper Authentication

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: Unknown

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommedations

The NCSC strongly reccommends installing updates for vulnerable systems with the highest priority, after thorough testing.

Affected organisations should review the latest release notes and install the relevant updates from Cobbler.

Please see following links for further information.

- https://github.com/cobbler/cobbler/security/advisories/GHSA-m26c-fcgh-cp6h
- https://github.com/cobbler/cobbler/commit/32c5cada013dc8daa7320a8eda9932c2814742b0
- https://github.com/cobbler/cobbler/commit/e19717623c10b29e7466ed4ab23515a94beb2dda