



CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

TLP:CLEAR

25 November 2024

Cobbler XML-RPC Authentication Bypass Vulnerability

CVE-2024-47533

Linux Installation

Unauthorized Access

Improper Authentication

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-47533. This vulnerability has a maximum CVSS 3.1 score of 9.8¹ and impacts Cobbler version 3.0.0 and any prior versions up to 3.2.3 and 3.3.7. Cobbler is an open-source Linux installation server that allows for the rapid deployment of network-based systems. The vulnerability consists of an improper authentication in which `utils.get_shared_secret()` always returns `-1`, allowing anyone to connect to Cobbler XML-RPC as user '' password `-1` and make any changes.² A successful exploitation gives malicious actors with network access to affected servers full control of the server. Proof of concept has been provided in Cobbler's security advisory.³

The Cal-CSIC recommends immediately upgrading to versions 3.2.3 and 3.3.7.

For further information on applying upgrades please refer to [Cobbler's Security Advisory](#).

Organization, Source, Reference, and Dissemination Information

Organization Description

California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

CAL-CSIC-202411-009

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

PUBLIC SERVICE ANNOUNCEMENT

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here .
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	Traffic Light Protocol (TLP): Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5

¹ National Vulnerability Database; “CVE-2024-47533 Detail”; <https://nvd.nist.gov/vuln/detail/CVE-2024-47533>; accessed 21 November 2024

² Vulners; “CVE-2024-47533”; <https://vulners.com/cve/CVE-2024-47533>; accessed 21 November 2024

³ Github; “Anyone can connect to cobbler XML-RPC server with known password and make changes”; <https://github.com/cobbler/cobbler/security/advisories/GHSA-m26c-fcgh-cp6h>; accessed 21 November 2024

CAL-CSIC-202411-009

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR