CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

2 January 2025

LDAP Remote Code Execution Vulnerability

CVE-2024-49112 | Proof-of-Concept | Integer Overflow | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of one critical vulnerability known as CVE-2024-49112 with a CVSS 3.x score of 9.8.[1] This vulnerability affects both Lightweight Directory Access Protocol (LDAP) clients and servers running on all Windows server versions prior to Microsoft's Security Updates December 2024.

Successful exploitation of this vulnerability results in an integer overflow that when exploited allows a remote attacker to conduct remote code execution (RCE). A Proof-of-Concept is published, however there are no known instances of this being weaponized and exploited in the wild.[2, 3]

If updating to the latest version is not possible, configure domain controllers to either not access the internet or not allow inbound RPC from untrusted networks. While either mitigation protects systems from this vulnerability, applying both configurations provides an effective defense-in-depth against this vulnerability.

The Cal-CSIC recommends immediately updating the affected window servers to the latest Security Update.

For a more in-depth look at the Proof-of-Concept please refer to the SafeBreach researcher's GitHub page.

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

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.

	cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
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-2024-49112 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-49112; accessed 2 January 2025

[2] GitHub; "CVE-2024-49113" https://github.com/SafeBreach-Labs/CVE-2024-49113; accessed 2 January 2025

[3] SafeBreach; "LDAPNightmare: SafeBreach Labs Publishes First Proof-of-Concept Exploit for CVE-2024-49113" https://www.safebreach.com/blog/ldapnightmare-safebreach-labs-publishes-first-proof-of-concept-exploit-for-cve-2024-49113/; accessed 2 January 2025

CAL-CSIC-202501-001

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

2