CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

10 April 2024

Windows Systems Rust Vulnerability

CVE-2024-24576 | Rust | Windows | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware a highly critical vulnerability known as CVE-2024-24576.[1] The vulnerability lies within the Rust standard library prior to version 1.77.2.[2] Additionally, the vulnerability is specific to Rust when running on Windows systems.[3] Exploitation of the vulnerability may allow an attacker to execute arbitrary code disguised as arguments to the command. This vulnerability may also affect the application that executes commands without specifying the file extension.[4]

The Cal-CSIC recommends immediately upgrading to Rust version 1.77.2.

For further information on applying the Rust upgrade, refer to Rust Blog.

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.
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 calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

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.

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] Cert EU; "Critical Vulnerability in Rust on Windows;" https://cert.europa.eu/publications/security-advisories/2024-035/; accessed 10 April 2024

[2] Tuari; "Rust Security Advisory CVE-2024-24576;" https://beta.tauri.app/blog/cve-2024-24576/; accessed 10 April 2024

[3] The Hacker News; "Critical 'BatBadBut' Rust Vulnerability Exposes Windows Systems to Attacks;" https://thehackernews.com/2024/04/critical-batbadbut-rust-vulnerability.html; accessed 10 April 2024

[4] Rust Blog; "Security advisory for the standard library (CVE-2024-24576);" https://blog.rust-lang.org/2024/04/09/cve-2024-24576.html; accessed 10 April 2024

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.