CYBER ADVISORY

TLP:CLEAR

23 October 2024

Pac4j Deserialization Vulnerability

Pac4j-core | Security Framework | Deserialization | RCE

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of one critical vulnerability under active exploitation known as CVE-2023-25581.[1] Pac4j is a security framework for Java. The vulnerability affects systems that store externally controlled values in attributes of the `UserProfile` class from pac4j-core. It can be exploited by providing an attribute that contains a serialized Java object with a special prefix `{#sb64}` and Base64 encoding. This can lead to Remote Code Execution (RCE). Proof of Concept demonstrates the exploitation of the CVE-2023-25581 to conduct RCE.[2] Although a `RestrictedObjectInputStream` is in place, that puts some restriction on what classes can be deserialized, it still allows a broad range of java packages and potentially exploitable with different gadget chains.[3]

The Cal-CSIC recommends immediately updating to the latest Pac4J version.

For further information on applying updates please refer to Pac4J documentation.

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 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-2023-25581 Detail" https://nvd.nist.gov/vuln/detail/CVE-2023-25581; accessed 23 October 2024

[2] GitHub; "CVE-2023-25581" https://github.com/p33d/CVE-2023-25581; accessed 23 October 2024

[3] Github Security Lab; "Java deserialization leading to RCE in pac4j-core - CVE-2023-25581" https://securitylab.github.com/advisories/GHSL-2022-085_pac4j/; accessed 23 October 2024