CYBER ADVISORY

TLP:CLEAR

09 April 2024

Multiple SAP Vulnerabilities

CVE-2024-27899 | CVE-2024-25646 | CVE-2024-27901 | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware high vulnerabilities known as CVE-2024-27899, CVE-2024-25646, and CVE-2024-27901.[1] CVE-2024-27899 affects the SAP NetWeaver AS Java User Management Engine. Exploitation may allow an attacker to cause profound impact on confidentiality and low impact on both integrity and availability.[2] CVE-2024-25646 affects SAP BusinessObjects Web Intelligence, Versions - 4.2, 4.3. Exploitation of the vulnerability may allow an attacker affect considerable impact on confidentiality of the application.[3] CVE-2024-27901 affects SAP Asset Accounting, Versions - SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_FIN617, SAP_FIN 618, SAP_FIN700. Exploitation of the vulnerability could allow a high privileged attacker to exploit insufficient validation of path information provided by the users and pass it through to the file API's.[4]

The Cal-CSIC recommends upgrading the affected SAP software to the appropriate patched version as soon as possible.

For further information on applying SAP upgrades, refer to SAP Upgrade Maintenance.

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.
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] Security Week; "SAP's April 2024 Updates Patch High-Severity Vulnerabilities;" https://www.securityweek.com/saps-april-2024-updates-patch-high-severity-vulnerabilities/; accessed 09 April 2024
[2] CVE.ORG; "CVE-2024-27899;" https://www.cve.org/CVERecord?id=CVE-2024-27899; accessed 09 April 2024
[3] CVE.ORG; "CVE-2024-25646;" https://www.cve.org/CVERecord?id=CVE-2024-25646; accessed 09 April 2024
[4] CVE.ORG; "CVE-2024-27901;" https://www.cve.org/CVERecord?id=CVE-2024-27901; accessed 09 April 2024