Advisory Alert

Alert Number: AAA20231010 **Date:** October 10, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42474, CVE-2023-40310, CVE-2023-42477, CVE-2023-42473, CVE-2023-31405, CVE-2023-31405, CVE-2023-41365, CVE-2023-42475)
Description	SAP has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Cross-Site Scripting (XSS), Missing XML Validation, Server-Side Request Forgery, Log Injection, and Information Disclosure. SAP recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	SAP BusinessObjects Web Intelligence, Versions–420 SAP PowerDesigner Client, Version –16.7 SAP NetWeaver AS Java, Version –7.50 S/4HANA (Manage Withholding Tax Items),Version –106 SAP NetWeaver AS for Java (Log Viewer), Version -ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50 SAP Business One (B1i), Version –10 SAP S/4HANA Core,Version –S4CORE 102, S4CORE 103, S4CORE 104, S4CORE 105,S4CORE 106, SAPSCORE 128
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.