Alerta de seguridad cibernética	9VSA23-00900-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2023
Última revisión	14 de septiembre de 2023

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de las vulnerabilidades incluidas en el más reciente boletín de actualizaciones de seguridad de SAP, correspondiente a septiembre de 2023.

Vulnerabilidades

CVE-2023-40622	CVE-2023-40308	CVE-2021-41183	CVE-2023-37489
CVE-2022-41272	CVE-2023-40621	CVE-2021-41182	CVE-2023-41369
CVE-2023-25616	CVE-2023-40623	CVE-2023-24998	CVE-2023-41368
CVE-2023-40309	CVE-2023-40306	CVE-2023-40624	CVE-2023-41367
CVE-2023-42472	CVE-2021-41184	CVE-2023-40625	

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-40622: Vulnerabilidad de revelación de información en la Business Intelligence Platform (Promotion Management) de SAP Business Objects. CVSS: 9.9.

CVE-2022-41272: Actualización de lo informado en el Patch Day de Diciembre 2022. Vulnerabilidad de control de acceso inapropiado en SAP NetWeaver AS Java (User Defined Seach). CVSS: 9.9.

CVE-2023-25616: Vulnerabilidad de inyección de código en SAP Business Objects Business Intelligence Platform (CMC). CVSS: 9.9.

CVE-2023-40309: Vulnerabilidad de chequeos de autenticación mal implementados o no implementados, en SAP CommonCryptoLib. CVSS: 9.8.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

SAP Business Client, Versiónes -6.5, 7.0, 7.70
SAP BusinessObjects Business Intelligence Platform (Promotion Management), versiones 420,430
SAP NetWeaver Process Integration, Versión –7.50
SAP Business Objects Business Intelligence Platform (CMC), versiones 420, 430
SAP CommonCryptoLib, Versiónes–8
SAP NetWeaver AS ABAP
SAP NetWeaver AS Java and ABAP Platform of S/4HANA on-premise.
SAP Web Dispatcher, Versiónes -7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89
SAP Content Server, Versiónes -6.50, 7.53, 7.54
SAP HANA Database, Versiónes –2.0
SAP Host Agent, Versiónes –722
SAP Extended Application Services and Runtime (XSA)
SAPSSOEXT, Versiónes –17
SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface),Versión 420
SAP CommonCryptoLib, Versiónes–8
SAP NetWeaver AS ABAP
SAP NetWeaver AS Java and ABAP Platform of S/4HANA on-premise.
SAP Web Dispatcher, Versiónes -7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89
SAPContent Server, Versiónes -6.50, 7.53, 7.54
SAPHANA Database, Versiónes –2.0
SAPHost Agent, Versiónes –722
SAPExtended Application Services and Runtime (XSA), versiones SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00
SAPSSOEXT, Versiónes –17
SAP PowerDesignerClient, Versión –16.7
SAP BusinessObjects Suite (Installer),Versión –420, 430
SAP S/4HANA (Manage Catalog Items and Cross-Catalog search), versiones S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106
SAPUI5, Versiónes –SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756, UI_700 200
SAP Quotation Management Insurance (FS-QUO), versiones 400, 510, 700, 800
SAP NetWeaver AS ABAP (applications based on Unified Rendering), versiones SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 702, SAP_BASIS 731
S4CORE (Manage Purchase Contracts App), Versiónes–102, 103, 104, 105, 106, 107
SAP BusinessObjects Business Intelligence Platform (Versión Management System), versiones 430
SAP NetWeaver (Guided Procedures), Versión –7.50
SAP S/4HANA (Create Single Payment application), versiones 100, 101, 102, 103, 104, 105, 106, 107, 108
S4 HANA ABAP (Manage checkbook apps), versiones 102, 103, 104, 105, 106, 107

Enlaces

https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40622

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41272
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25616
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40308
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40623
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40306
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24998
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40625
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37489
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41369
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41368
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41367

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.14 17:01:03 -03'00'