Alerta de seguridad cibernética	9VSA23-00862-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2023
Última revisión	13 de julio 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 nuevas vulnerabilidades parchadas por SAP en varios de sus productos, como parte de su SAP Security Patch Day, Julio 2023.

Vulnerabilidades

CVE-2023-36922	CVE-2023-35871	CVE-2023-35870	CVE-2023-35874
CVE-2023-33989	CVE-2023-36925	CVE-2023-33988	CVE-2023-36917
CVE-2023-33987	CVE-2023-36921	CVE-2023-36918	CVE-2023-31405
CVE-2023-33991	CVE-2023-35873	CVE-2023-36920	CVE-2023-36924
CVE-2023-33990	CVE-2023-35872	CVE-2023-36919	CVE-2023-33992

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-36922: Vulnerabilidad de inyección de comandos OS en SAP ECC y SAP S/4HANA (IS-OIL). Puntaje CVSS: 9.1.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

SAP ECC and SAP S/4HANA (IS-OIL) versiones 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807.
SAP Business Client, Versions -6.5, 7.0, 7.70.
SAP NetWeaver (BI CONT ADD ON), Versions –707, 737, 747, 757
SAP UI5 Variant Management, Versions –SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200.
SAP SQL Anywhere, Version-17.0.

SAP Solution Manager (Diagnostic Agent), Versions –7.20.
SAP NetWeaver Process Integration (Runtime Workbench), Versions–SAP_XITOOL 7.50.
SAP NetWeaver Process Integration (Message Display Tool), Versions–SAP_XIAF 7.50.
SAP NetWeaver AS ABAP and ABAP Platform, Version -KRNL64NUC7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL7.53, KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.92, KERNEL 7.93.
SAP BusinessObjects BI Platform (Enterprise),Version -4.20, 430.
SAP NetWeaver AS for Java (Log Viewer), Version -ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50.
SAP ERP Defense Forces and Public Security, Version -600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807.
SAP Business Warehouseand SAP BW/4HANA, Version -SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300.
SAP Web Dispatcher, Versions–WEBDISP 7.49, WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.81, WEBDISP 7.85, WEBDISP 7.88, WEBDISP 7.89, WEBDISP 7.90, KERNEL 7.49, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.88, KERNEL 7.89, KERNEL 7.90, KRNL64NUC 7.49, KRNL64UC 7.49, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1
SAP S/4HANA (Manage Journal Entry Template), Versions–S4CORE 104, 105, 106, 107.
SAP Enable Now, Version -WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704.

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-2023-36922
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35871
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36925
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36921
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35873
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35872
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35870
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36918
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36920
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36919
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-35874
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36917
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-31405
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36924

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33992

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.12 16:42:24 -04'00'