Alerta de seguridad cibernética	9VSA23-00877-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	8 de agosto de 2023
Última revisión	8 de agosto 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 vulnerabilidades parchadas por SAP como parte de su SAP Security Patch Day de agosto 2023.

Vulnerabilidades

CVE-2023-37484
CVE-2023-37483
CVE-2023-36922
CVE-2023-39439
CVE-2023-33989
CVE-2023-36923
CVE-2023-39437
CVE-2023-37490
CVE-2023-37491
CVE-2023-33993
CVE-2023-37488
CVE-2023-37486
CVE-2023-39436
CVE-2023-37487
CVE-2023-37492
CVE-2023-39440
CVE-2023-36926

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-37484 y CVE-2023-37483: Vulnerabilidades en SAP PowerDesigner 16.7. CVSS: 9.8.

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

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

SAP PowerDesigner 16.7
SAP ECC and SAP S/4HANA (IS-OIL), Versions -600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807.
SAP Commerce, Versions –HY_COM 2105, HY_COM 2205, COM_CLOUD 2211.
SAP NetWeaver (BI CONT ADD ON), Versions –707, 737, 747, 757.
SAP Business One, Version –10.0

SAP Business One (Service Layer), Version –10.0
SAP Business One (B1i Layer), Version –10.0
SAP BusinessObjects Business Intelligence (installer), Versions –420, 430.
SAP Message Server, Versions–KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EX.
SAP Supplier Relationship Management, Versions –600, 602, 603, 604, 605, 606, 616, 617.
SAP NetWeaver Process Integration, Versions-SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50
SAP Commerce (OCC API), Versions-HY_COM 2105, HY_COM 2205, COM_CLOUD 2211.
SAP Supplier Relationship Management, Versions –600, 602, 603, 604, 605, 606, 616, 617.
SAP NetWeaver AS ABAP and ABAP Platform, Versions –SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804.

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-2023-37484
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37483
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36922
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36923
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39437
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37491
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37488
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37486
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39436
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37487
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39440
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36926

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.08.08 15:40:19 -04'00'