Alerta de seguridad cibernética	9VSA23-00768-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero 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 la información entregada por SAP sobre nuevas vulnerabilidades que afectan a varios de sus productos, y para las cuales pusieron a disposición actualizaciones de seguridad.

Vulnerabilidades

CVE-2022-41203
CVE-2022-41271
CVE-2022-41272
CVE-2023-0014
CVE-2023-0023
CVE-2023-0015
CVE-2023-0022
CVE-2023-0018
CVE-2023-0017
CVE-2023-0016
CVE-2023-0012
CVE-2023-0013

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-41203: Vulnerabiliad de deserialización insegura de datos no confiables en SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad) versiones 4.2, 4.3.

CVE-2022-41271: Vulnerabilidad de controles de acceso inapropiados en SAP NetWeaver Process Integration (Messaging System) versión 7.50.

CVE-2022-41272: Vulnerabilidad de controles de acceso inapropiados en SAP NetWeaver Process Integration (User Defined Search) versión 7.50.

CVE-2023-0014: Vulnerabilidad de tipo capture-replay en SAP NetWeaver ABAP Server and ABAP Platform, SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT.

CVE-2023-0022: Vulnerabilidad de inyección de código en SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP) versiones 420, 430.

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob

CVE-2023-0017: Vulnerabilidad de acceso inapropiado en SAP NetWeaver AS for Java, versión 7.50.

CVE-2023-0016: Vulnerabilidad de inyección SQL en SAP BPC MS 10.0 versiones 800, 810.

Productos afectados

SAP NetWeaver Process Integration (Messaging System) versión 7.50.
SAP NetWeaver Process Integration (User Defined Search) versión 7.50.
SAP NetWeaver ABAP Server and ABAP Platform
SAP BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT.
SAP NetWeaver AS for ABAP and ABAP Platform, versiones 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757.
SAP NetWeaver AS for Java, versión 7.50.
SAP BusinessObjects Business Intelligence Platform (Analysis edition for OLAP) versiones 420, 430.
SAP BusinessObjects Business Intelligence Platform (Central management console) versiones 420, 430.
SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad) versiones 4.2, 4.3.
SAP BusinessObjects Business Intelligence Platform, versión 420.
SAP BPC MS 10.0 versiones 800, 810.
SAP Host Agent (Windows), Versiones - 7.21, 7.22.
SAP Bank Account Management (Manage Banks) versiones 800, 900.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41203
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41271
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41272
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0013

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.11 17:20:22 -03'00'