Alerta de seguridad cibernética	9VSA23-00817-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2023
Última revisión	12 de abril 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 parchadas por SAP para SAP Diagnostics Agent y SAP BusinessObjects Business Intelligence Platform, tres críticas.

Vulnerabilidades

CVE-2023-27267
CVE-2023-28765
CVE-2023-29186

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-27267: Un error de insuficiente validación de entradas y falta de autenticación, que impacta el OSCommand Bridge del SAP Diagnostics Agent, versión 720, y que permite a un atacante ejecutar scripts en agentes conectados y comprometer totalmente el sistema.

CVE-2023-28765: Vulnerabilidad de revelación de información que impacta a la SAP BusinessObjetcs Intelligence Platform (Platform Management), versiones 420 y 430, permiten a un atacante con privilegios básicos ganar acceso al archivo Icmbiar y descifrarlo. Esto podría permitir a un atacante acceder a las contraselas de los usuarios de la plataforma y tomar control de sus cuentas para realizar acciones maliciosas adicionales.

CVE-2023-29186: Vulnerabilidad de tipo directory traversal que impacta a SAP NetWeaver 707, 737, 747 y 757, que permiten a un atacante cargar y sobreescribir archivos en un servidor SAP vulnerable.

Productos afectados

SAP Diagnostics Agent y SAP BusinessObjects Business Intelligence Platform

Enlaces

https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
https://nvd.nist.gov/vuln/detail/CVE-2023-29186
https://nvd.nist.gov/vuln/detail/CVE-2023-28765
https://nvd.nist.gov/vuln/detail/CVE-2023-27267
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29186
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27267

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.04.13 09:30:17 -04'00'