BOLETÍN DE ALERTA

Boletín Nro.: 2023-41
Fecha de publicación: 13/09/2023
Tema: Actualizaciones de seguridad para productos SAP

Principales softwares afectados:

- SAP BusinessObjects Business Intelligence Platform (Promotion Management), versiones 420 y 430.
- SAP CommonCryptoLib, versión 8.
- SAP HANA Database, versión 2.0.
- SAP PowerDesigner Client, versión 16.7.
- SAP BusinessObjects Suite (Installer), versiones 420 y 430.

Adicionalmente, puede acceder al listado completo de software afectado ingresando aquí.

Descripción:

Se ha reportado un aviso de seguridad sobre múltiples vulnerabilidades que afectan a productos SAP, que permitirían a un atacante obtener acceso no autorizado, realizar inyección de códigos, divulgación de información, entre otros.

Las vulnerabilidades corregidas se componen de 2 (dos) de severidad “Crítica”, 2 (dos) de severidad “Alta”, 7 (siete) de severidad “Media” y 2 (dos) de severidad “Baja”. Las principales se detallan a continuación:

- CVE-2023-40622, de severidad “Crítica” y con puntuación de 9.9. Esta vulnerabilidad se debe a una falla de seguridad SAP BusinessObjects Business Intelligence Platform (Promotion Management). Esto permitiría a un atacante autenticado obtener información confidencial, comprometer totalmente la aplicación afectada y causar un gran impacto en la confidencialidad, la integridad y la disponibilidad de la misma.

- CVE-2023-40309, de severidad “Crítica” y con puntuación de 9.8. Esta vulnerabilidad se debe a una falla de validación de autorización en SAP CommonCryptoLib. Esto permitiría a un atacante realizar omisión de autenticación, escalamiento de privilegios y dependiendo de la aplicación afectada y del nivel de privilegios obtenido, posteriormente leer, modificar o eliminar datos restringidos a un grupo de usuarios.

- CVE-2023-42472, de severidad “Alta” y con puntuación asignada de 8.7. Esta vulnerabilidad se debe a una falla de validación del tipo de archivo de datos en SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface). . Esto permitiría a un atacante autenticado a través de la red, subir archivos desde el sistema local, modificar el tipo de contenido y la información confidencial, la extensión para leer datos y causar un gran impacto en la confidencialidad, la integridad y la disponibilidad en la aplicación afectada.

Adicionalmente, puede acceder al listado completo de vulnerabilidades ingresando aquí.

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante obtener acceso no autorizado, realizar inyección de códigos, divulgación de información, entre otros.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través de la siguiente guía:

- https://support.sap.com/en/my-support/software-downloads.html?anchorId=section

Información adicional:

- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1712/
- https://nvd.nist.gov/vuln/detail/CVE-2023-40622
- https://nvd.nist.gov/vuln/detail/CVE-2023-40309
- https://nvd.nist.gov/vuln/detail/CVE-2023-42472
- https://www.sap.com/docs/download/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.pdf
- https://support.sap.com/en/my-support/software-downloads.html?anchorId=section