Basque CyberSecurity Centre

# Actualización de seguridad de SAP-Septiembre 2023

BCSC-ACTUALIZACIONES-SAP-2023-SEPTIEMBRE

**TLP: CLEAR**

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

## TABLA DE CONTENIDO



## Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

## Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

## Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.


El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

## 1. Resumen ejecutivo

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de septiembre para una amplia gama de sus productos. En total, se han notificado 18 nuevas notas de seguridad, a las que se añaden 1 actualizaciones de notas publicadas con anterioridad. De todas ellas, 5 se clasifican como de severidad crítica, 2 alta,  9 media y 2 bajas, corrigiendo fallos de denegación de servicio, Cross-Site Scripting (XSS), corrupción de memoria e inyección de comandos del sistema operativo, entre otros.

En cuanto a las vulnerabilidades de mayor impacto tratadas en esta actualización afectan principalmente a los productos SAP BusinessObjects Business Intelligence Platform y SAP CommonCryptoLib.

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

## 2. Recursos afectados

Las actualizaciones de seguridad del mes de Septiembre de 2023 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- SAP Business Client, versiones 6.5, 7.0, 7.70.
- SAP ECC y SAP S/4HANA (IS-OIL), versiones 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807.
- SAP NetWeaver (BI CONT ADD ON), versiones 707, 737, 747, 757.
- SAP Web Dispatcher, versiones 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_SERVICES1.
- SAP UI5 Variant Management, versiones 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), versión 7.20.
- SAP NetWeaver Process Integration (Runtime Workbench), versión SAP_XITOOL 7.50.
- SAP NetWeaver Process Integration (Message Display Tool), versión SAP_XIAF 7.50.
- SAP S/4HANA (Manage Journal Entry Template), versiones S4CORE 104, 105, 106, 107.
- SAP NetWeaver AS ABAP y ABAP Platform, versiones KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC, 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL 7.53, 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), versiones 4.20, 430.
- SAP NetWeaver AS para Java (Log Viewer), versiones ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50.
- SAP ERP Defense Forces and Public Security, versiones 600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807.
- SAP Business Warehouse and SAP BW/4HANA, versiones SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300.

## 3. Análisis técnico

A continuación, se detalla la lista con todas las vulnerabilidades identificadas:

| Nota de seguridad | Severidad | CVSS |
|---|---|---|
| **Nota 2622660**<br><br>Actualización de la nota de seguridad publicada en abril de 2018 que se corresponde con actualizaciones de seguridad para el control del navegador Google Chromium en SAP Business Client. | **Crítica** | 10.0 |
| **Nota 3320355**<br><br>CVE-2023-40622: vulnerabilidad de divulgación de información en SAP BusinessObjects Business Intelligence Platform (Gestión de promociones). | **Crítica** | 9.9 |
| **Nota 3273480**<br><br>CVE-2022-41272: vulnerabilidad de inyección de código en SAP Business Objects Business Intelligence Platform (CMC). | **Crítica** | 9.9 |
| **Nota 3245526**<br><br>CVE-2023-25616: vulnerabilidad de inyección de código en SAP Business Objects Business Intelligence Platform (CMC) | **Crítica** | 9.9 |
| **Nota 3340576**<br><br>CVE-2023-40309: falta la verificación de autorización en SAP CommonCryptoLib. | **Crítica** | 9.8 |
| **Nota 3370490**<br><br>CVE-2023-42472: validación de tipo de archivo insuficiente en la plataforma SAP BusinessObjects Business Intelligence (interfaz HTML de Web Intelligence). | Alta | 8.7 |
| **Nota 3327896**<br><br>CVE-2023-40308: vulnerabilidad de corrupción de memoria en SAP CommonCryptoLib. | Alta | 7.5 |
| **Nota 3357163**<br><br>CVE-2023-40621: vulnerabilidad de inyección de código en el cliente SAP PowerDesigner. | Media | 6.3 |
| **Nota 3317702** | Media | 6.2 |

| | | |
|---|---|---|
| CVE-2023-40623: eliminación arbitraria de archivos a través de Directory Junction en SAP BusinessObjects Suite (instalador). | | |
| **Nota 3156972**<br><br>CVE-2023-40306: vulnerabilidad de redireccionamiento de URL en SAP S/4HANA (administrar elementos del catálogo y búsqueda entre catálogos). | Media | 6.1 |
| **Nota 3149794**<br><br>CVE-2021-41182: XSS en la opción `altField` del widget Datepicker. | Media | 6.1 |
| **Nota 3349805**<br><br>CVE-2023-24998: apache Commons FileUpload, Apache Tomcat: FileUpload DoS. | Media | 5.7 |
| **Nota 3323163**<br><br>CVE-2023-40624: vulnerabilidad de inyección de código en SAP NetWeaver AS ABAP (aplicaciones basadas en Unified Rendering). | Media | 5.5 |
| **Nota 3326361**<br><br>CVE-2023-40625: falta la verificación de autorización en la aplicación SAP Manage Purchase Contracts. | Media | 5.4 |
| **Nota 3352453**<br><br>CVE-2023-37489: vulnerabilidad de divulgación de información en SAP BusinessObjects Business Intelligence Platform (Sistema de gestión de versiones). | Media | 5.3 |
| **Nota 3348142**<br><br>CVE-2023-41367: falta verificación de autenticación en SAP NetWeaver (procedimientos guiados). | Media | 5.3 |
| **Nota 3369680**<br><br>CVE-2023-41369: vulnerabilidad de bucle de entidad externa en SAP S/4HANA (Crear aplicación de pago único). | Baja | 3.5 |
| **Nota 3355675**<br><br>CVE-2023-41368: vulnerabilidad de referencia directa a objetos inseguros (IDOR) en S4 HANA. | Baja | 2.7 |

## 4. Mitigación / Solución

Con el fin de mitigar y corregir cualquier vulnerabilidad, SAP publica mensualmente información sobre las notas de seguridad en su página web.

## 5. Referencias Adicionales

- SAP Security Patch Day – September 2023.


EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA