Basque CyberSecurity Centre

Actualización de seguridad de SAP-Marzo 2023

BCSC-ACTUALIZACIONES-SAP-2023-MARZO

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 marzo para una amplia gama de sus productos. En total, se han notificado 19 nuevas notas de seguridad de las cuales 5 se clasifican como críticas, 4 altas y 10 como medias, corrigiendo fallos de ejecución remota de código, denegación de servicio, inyección de entidad externa XML (XXE), Cross-Site Scripting (XSS) y divulgación de información, entre otras.

Por otra parte, las vulnerabilidades críticas tratadas en esta actualización afectan a los productos SAP Business Objects Business Intelligence Platform, SAP NetWeaver AS para Java, SAP NetWeaver AS para ABAP y ABAP Platform y SAP ERP y S4HANA.

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 marzo de 2023 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- SAP Business Objects Business Intelligence Platform (CMC), versiones 420, 430.
- SAP NetWeaver AS para Java, versión 7.50.
- SAP NetWeaver Application Server para ABAP y ABAP Platform, versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791.
- SAP NetWeaver AS para ABAP y ABAP Platform (SAPRSBRO Program), versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757.
- SAP Business Objects (Adaptive Job Server), versiones 420, 430.
- SAP Solution Manager y ABAP managed systems (ST-PI), versiones 2008_1_700, 2008_1_710 y 740.
- SAP NetWeaver AS para ABAP y ABAP Platform, versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791.
- SAP Host Agent, versión 7.22.
- SAP NetWeaver (SAP Enterprise Portal), versión 7.50.
- SAP ABAP Platform, versiones 751, 753, 753, 754, 756, 757, 791.
- SAP NetWeaver Application Server para ABAP y ABAP Platform, versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791.
- SAP BusinessObjects Business Intelligence Platform (Web Services), versiones 420, 430.
- SAP Content Server, versión 7.53.
- SAP Authenticator para Android, versión 1.3.0.
- SAP NetWeaver, versiones 700, 701, 702, 731, 740, 750.
- SAP NetWeaver AS Java (Object Analyzing Service), versión 7.50.
- SAP NetWeaver AS Java, versión 7.50.

3. Análisis técnico

Los detalles de las vulnerabilidades más relevantes corregidas en esta actualización son los siguientes:

CVE-2023-25616**:** vulnerabilidad de inyección de código de forma que, en algunos escenarios en SAP Business Objects Business Intelligence Platform (CMC) en las versiones 420, 430, la ejecución de objetos de programa puede provocar este fallo lo que podría permitir que un atacante obtuviese acceso a los recursos permitidos por privilegios adicionales. Un ataque exitoso podría tener un gran impacto en la confidencialidad, la integridad y la disponibilidad del sistema.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.9

CWE 74: Improper Neutralization of Special Elements in Output Used by a Downstream Component (Injection)

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-23857**:** vulnerabilidad de control de acceso inadecuado debida a la falta de verificación de autenticación en SAP NetWeaver AS para Java en la versión 7.50, que permite que un atacante no autenticado se conecte a una interfaz abierta y haga uso de una API abierta de nombres y directorios para acceder a servicios que pueden usarse para realizar operaciones no autorizadas que afectan a usuarios y servicios a través de los sistemas. En una explotación exitosa, el atacante podría leer y modificar cierta información confidencial, pero también puede usarse para bloquear cualquier elemento u operación del sistema, lo que hace que no responda o no esté disponible.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.9

CWE 287: Improper Authentication

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H

- **Vector de ataque**: **Red**

- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Baja
- **Integridad:** Baja
- **Disponibilidad: Alta**

CVE-2023-27269**:** vulnerabilidad de falta de autorización en SAP NetWeaver Application Server para ABAP y ABAP Platform que permite a un atacante con autorizaciones no administrativas explotar un defecto de recorrido de directorio en un servicio disponible para sobrescribir los archivos del sistema. En este ataque, no se pueden leer datos, pero los archivos del sistema operativo potencialmente críticos se pueden sobrescribir, lo que hace que el sistema no esté disponible**.**

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.6

CWE 862: Missing Authorization

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-27500**:** vulnerabilidad de limitación incorrecta de un nombre de ruta a un directorio restringido (Path Traversal) de manera que, un atacante con autorizaciones no administrativas puede explotar un fallo de cruce de directorios en el programa SAPRSBRO para sobrescribir los archivos del sistema. En este ataque, no se pueden leer datos, pero los archivos del sistema operativo potencialmente críticos se pueden sobrescribir, lo que hace que el sistema no esté disponible.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.6

CWE 22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-25617**:** vulnerabilidad de ejecución de comandos del sistema operativo en SAP Business Object (Adaptive Job Server) versiones 420, 430, que permite la ejecución remota de comandos arbitrarios en Unix, cuando la ejecución de objetos de programa está habilitada, para usuarios autenticados con derechos de programación, utilizando BI Launchpad, Central Management Console o una aplicación personalizada basada en el SDK público de Java. Los programas podrían afectar la confidencialidad, la integridad y la disponibilidad del sistema.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.0

CWE 74: Improper Neutralization of Special Elements in Output Used by a Downstream Component (Injection)

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: Requerida
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

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

Nota de seguridad	Severidad	CVSS
Nota 3245526 CVE-2023-25616: vulnerabilidad de inyección de código en SAP Business Objects Business Intelligence Platform (CMC)**.**	**Crítica**	9.9
Nota 3252433 CVE-2023-23857: vulnerabilidad de control de acceso inadecuado en SAP NetWeaver AS para Java.	**Crítica**	9.9

Nota 3294595 CVE-2023-27269: vulnerabilidad de falta de autorización en SAP NetWeaver AS para ABAP y Plataforma ABAP.	**Crítica**	9.6
Nota 3302162 CVE-2023-27500: vulnerabilidad de limitación incorrecta de un nombre de ruta a un directorio restringido (Path Traversal) en SAP ERP y S4HANA (Programa SAPRSBRO).	**Crítica**	9.6
Nota 3283438 CVE-2023-25617: vulnerabilidad de ejecución de comandos del sistema operativo en SAP Business Objects Business Intelligence Platform (Adaptive Job Server).	**Crítica**	9.0
Nota 3296476 CVE-2023-27893: vulnerabilidad de ejecución de código arbitrario en SAP Solution Manager y sistemas gestionados ABAP (ST-PI).	Alta	8.8
Nota 3294954 CVE-2023-27501: vulnerabilidad de Directory Traversal en SAP NetWeaver AS para ABAP y Plataforma ABAP.	Alta	8.7
Nota 3296346 CVE-2023-26459**:** Múltiples vulnerabilidades en SAP NetWeaver AS para ABAP y Plataforma ABAP. CVE adicional CVE-2023-25618.	Alta	7.4
Nota 3275727 CVE-2023-27498: vulnerabilidad de Corrupción de Memoria en SAPOSCOL.	Alta	7.2
Nota 3284550 CVE-2023-26461: vulnerabilidad XXE en SAP NetWeaver (SAP Enterprise Portal).	Media	6.8
Nota 3289844 CVE-2023-25615: vulnerabilidad de inyección SQL en plataforma ABAP.	Media	6.8
Nota 3296328 CVE-2023-27270: vulnerabilidad de denegación de servicio (DoS) en SAP NetWeaver AS para ABAP y Plataforma ABAP.	Media	6.5

Nota 3287120 Múltiples vulnerabilidades en la plataforma SAP BusinessObjects Business Intelligence. • CVE-2023-27271: vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF). • CVE-2023-27896: vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF). • CVE-2023-27894: vulnerabilidad de exposición de información confidencial a un actor no autorizado.	Media	6.5
Nota 3281484 CVE-2023-26457: vulnerabilidad de Cross-Site Scripting (XSS) en SAP Content Server.	Media	6.1
Nota 3302710 CVE-2023-27895: vulnerabilidad de divulgación de información en SAP Authenticator para Android.	Media	6.1
Nota 3274920 CVE-2023-0021: vulnerabilidad de Cross-Site Scripting (XSS) en SAP NetWeaver.	Media	6.1
Nota 3288480 CVE-2023-27268: vulnerabilidad de falta verificación de autenticación y autorización en SAP NetWeaver AS Java (Servicio de análisis de objetos).	Media	5.3
Nota 3288096 CVE-2023-26460: vulnerabilidad de falta verificación de autenticación en SAP NetWeaver AS para Java (Servicio de administración de caché).	Media	5.3
Nota 3288394 CVE-2023-24526: vulnerabilidad de control de acceso inadecuado en SAP NetWeaver AS Java (Classload Service).	Media	5.3

4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades, SAP publica información sobre las notas de seguridad publicadas mensualmente en su página web.

5. Referencias Adicionales

- SAP Security Patch Day – March 2023.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA