Actualización de seguridad de SAP-Abril 2024

CYBERZAINTZA- ACTUALIZACIONES-SAP-2024-ABRIL

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca. 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.

1. Resumen ejecutivo

SAP ha publicado las actualizaciones de seguridad correspondientes al mes de abril para una amplia gama de sus productos. En total, se han notificado **10 nuevas notas de seguridad** con **2 actualizaciones** de notas publicadas con anterioridad. De todas ellas, **3** se clasifican como **severidad alta** y **9** como **severidad media**, corrigiendo fallos de configuración incorrecta, divulgación de información, errores transversales de directorios, denegación de servicio (DDoS), Cross-Site Scripting (XSS) y divulgación de información, entre otros.

Respecto a las notas de seguridad de mayor impacto abordadas en esta actualización, afectan a los productos **SAP NetWeaver**, **SAP BusinessObjects Web Intelligence** y **SAP Asset Accounting,** siendo todas ellas una amenaza de alta gravedad para la confidencialidad de los sistemas que se puedan ver afectados.

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 abril de 2024 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- SAP NetWeaver AS Java User Management Engine, versiones SERVERCORE 7.50, J2EE-APPS 7.50, UMEADMIN 7.50.
- SAP BusinessObjects Web Intelligence, versiones 4.2 y 4.3.
- SAP Asset Accounting, versiones SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_APPL 600, SAP_FIN617, SAP_FIN 618, SAP_FIN700.
- SAP Edge Integration Cell, versiones anteriores a la versión 8.13.5.
- SAP NetWeaver AS ABAP and 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 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.93.
- SAP Group Reporting Data Collection (Enter Package Data), versiones S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, SAP_GRDC_CLOUD 1.0.0.
- SAP Employee Self Service (Fiori My Leave Request), versión 605.
- SAP S/4HANA (Manage Catalog Items and Cross-Catalog search), versiones S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106.
- SAP NetWeaver, versión 7.50.
- SAP Business Connector, versión 4.8.
- SAP S/4 HANA (Cash Management), versiones S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108.
- SAP S/4 HANA (Cash Management), versiones S4CORE 106, S4CORE 107, S4CORE 108.

3. Análisis técnico

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

CVE-2024-27899: vulnerabilidad debida a que el proceso de auto-registro y modificación del perfil propio en la aplicación de administración de usuarios de NetWeaver AS Java no cumple con los requisitos de seguridad necesarios para la gestión de la respuesta de seguridad recién establecida. Esta vulnerabilidad puede ser aprovechada por un atacante para provocar un serio impacto en la confidencialidad, así como un menor impacto en la integridad y disponibilidad de los datos.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-640: Weak Password Recovery Mechanism for Forgotten Password

CVSS Base: **8.8**

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

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

CVE-2024-25646: debido a una validación inadecuada, SAP BusinessObject Business Intelligence Launch Pad permite que un atacante autenticado acceda a la información del sistema operativo mediante la manipulación de documentos. En caso de explotación exitosa, esto podría tener un impacto significativo en la confidencialidad de la aplicación.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

CVSS Base: **7.7**

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

- **Vector de Ataque: Red**
- **Complejidad de ataque: Baja**
- **Privilegios requeridos: Bajos**
- **Interacción del usuario: Ninguna**
- **Alcance: Con cambios**

- **Confidencialidad: Alta**
- **Integridad:** Ninguna
- **Disponibilidad:** Ninguna

CVE-2024-27901: SAP Asset Accounting podría permitir que un atacante con altos privilegios aproveche la validación insuficiente de la información de la ruta proporcionada por los usuarios y la pase a través de las API de archivos. Esto podría causar un impacto considerable en la confidencialidad, integridad y disponibilidad de la aplicación.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-35: Path Traversal

CVSS Base: **7.2**

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

- **Vector de Ataque: Red**
- **Complejidad de ataque: Baja**
- **Privilegios requeridos:** Altos
- **Interacción del usuario: Ninguno**
- **Alcance:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

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

Nota	Descripción	Severidad	CVSS
3434839	**CVE-2024-27899**: vulnerabilidad en la aplicación de administración de usuarios de NetWeaver AS Java, donde el auto-registro y la modificación de perfiles no aplican los requisitos de seguridad necesarios para las respuestas de seguridad.	Alta	8.8
3421384	**CVE-2024-25646**: vulnerabilidad debida a la falta de validación en SAP BusinessObject Business Intelligence Launch Pad permite que un atacante autenticado acceda a información del sistema operativo a través de un documento manipulado.	Alta	7.7
3438234	**CVE-2024-27901**: vulnerabilidad causada por la insuficiente	Alta	7.2

	validación de la información de ruta en SAP Asset Accounting que podría ser explotada para acceder a las API de archivos.		
3359778	CVE-2024-30218: vulnerabilidad en el servidor de aplicaciones ABAP de SAP NetWeaver, así como la Plataforma ABAP que permiten a un atacante evitar que los usuarios legítimos accedan a un servicio, ya sea mediante su colapso o inundación. Esto provoca un impacto considerable en la disponibilidad.	Media	6.5
3442378	CVE-2024-28167: vulnerabilidad causada porque la recopilación de datos de SAP Group Reporting no verifica adecuadamente la autorización para usuarios autenticados, lo que permite una escalada de privilegios. Esto permite a usuarios no autorizados modificar datos específicos a través de la aplicación Enter Package Data, causando un impacto importante en la integridad de la aplicación.	Media	6.5
3164677	CVE-2022-29613: vulnerabilidad causada por una validación insuficiente de la entrada, SAP Employee Self Service permite a un atacante autenticado con privilegios de usuario alterar el número de empleado. En caso de explotación exitosa, el atacante puede ver los detalles personales de otros usuarios, lo que provoca un impacto limitado en la confidencialidad de la aplicación.	Media	6.5
3156972	CVE-2023-40306: vulnerabilidad que afecta a las aplicaciones Fiori de SAP S/4HANA, "Manage Catalog Items" y "Cross-Catalog searches", permiten a un atacante redirigir a los usuarios a un sitio	Media	6.1

	malicioso debido a una validación insuficiente de las URL.		
3425188	CVE-2024-27898: vulnerabilidad causada por una validación insuficiente de la entrada debido a este hecho, una aplicación de SAP NetWeaver permite a un atacante enviar una solicitud manipulada desde una aplicación web vulnerable dirigida a sistemas internos detrás de cortafuegos que normalmente son inaccesibles para un atacante desde la red externa, lo que resulta en una vulnerabilidad de Falsificación de Solicitudes del Lado del Servidor (Server-Side Request Forgery). Esto tiene un impacto bajo en la confidencialidad.	Media	5.3
3421453	CVE-2024-30214, CVE-2024-30215: vulnerabilidades de tipo XSS en SAP Business Connector.	Media	4.8
3427178	CVE-2024-30216**:** vulnerabilidad cuyo origen radica en el módulo de Gestión de Efectivo en SAP S/4 HANA, el cual no realiza las comprobaciones de autorización necesarias para un usuario autenticado, lo que resulta en una escalada de privilegios.	Media	4.3
3430173	CVE-2024-30217**:** vulnerabilidad generada en SAP S/4 HANA debido a que no lleva a cabo las comprobaciones de autorización necesarias para un usuario autenticado, lo que resulta en una escalada de privilegios.	Media	4.3

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 – April 2024.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY