Actualización de seguridad de SAP-Marzo 2024

CYBERZAINTZA- ACTUALIZACIONES-SAP-2024-MARZO

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 marzo 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 crítica**, **3** como **severidad alta**, y **6** como **severidad media**, corrigiendo fallos de inyección de código malicioso, autenticación incorrecta, denegación de servicio (DDoS), recorrido de ruta, Cross-Site Scripting (XSS), divulgación de información y falta verificación de autorización.

Respecto a las notas de seguridad de mayor impacto abordadas en esta actualización, la primera se centra en el producto SAP Business Client, que hereda vulnerabilidades ya tratadas en la nota de seguridad publicada en abril de 2018 provenientes del navegador Google Chromium. Las dos restantes impactan en los productos **SAP Build Apps** y **SAP NetWeaver AS Java**.

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

- SAP Business Client, versiones 6.5, 7.0, 7.70.
- SAP Build Apps, versiones < 4.9.145.
- SAP NetWeaver AS Java (Administrator Log Viewer plug-in), versión 7.50.
- SAP Commerce, versiones HY_COM 2105, HY_COM 2205, COM_CLOUD 2211.
- SAP HANA Database, versión 2.0.
- SAP HANA Extended Application Services Advanced (XS Advanced), versión 1.0.
- SAP BusinessObjects Business Intelligence Platform (Central Management Console), versiones 4.3.
- SAP NetWeaver AS ABAP applications basado en SAPGUI para HTML(WebGUI), versiones 7.89, 7.93.
- NetWeaver (WSRM), versiones 7.50.
- SAP NetWeaver (Enterprise Portal), versión 7.50.
- SAP NetWeaver Process Integration (Support Web Pages), versiones 7.50.
- SAP Fiori Front End Server, versión 605.
- SAP ABAP Platform, versiones 758, 795.

3. Análisis técnico

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

La nota de seguridad **2622660**, publicada en abril de 2018, tiene como objetivo actualizar a los clientes de productos SAP sobre las vulnerabilidades que SAP Business Client hereda de navegadores web de terceros, como Google Chromium. Las vulnerabilidades enumeradas en la nota de seguridad se encuentran en componentes entregados por Google y la información sobre las actualizaciones publicadas por Google se encuentran disponibles en: Chrome 63, Chrome 64, Chrome 65.

CVE-2019-10744: vulnerabilidad de inyección de código que afecta a SAP Build Apps en versiones anteriores a la versión 4.9.145. La biblioteca lodash de javascript en versiones anteriores a la versión 4.17.12 pueden verse afectadas por la vulnerabilidad "*prototipe pollution*", cuya explotación permite agregar propiedades arbitrarias a los prototipos de objetos globales.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

CVSS Base: **9.4**

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

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

CVE-2024-22127: vulnerabilidad de inyección de código que afecta a SAP NetWeaver AS Java en su versión 7.50. La explotación exitosa de esta vulnerabilidad posibilitaría, a un atacante con privilegios elevados, la carga de archivos potencialmente peligrosos, lo que le permitiría ejecutar comandos que pueden tener un alto impacto en la confidencialidad, la integridad y disponibilidad de la aplicación.

La métrica de evaluación de las vulnerabilidades se compone de:

CVSS Base: **9.1**

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

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

CVE-2023-39439: vulnerabilidad de autenticación impropia que afecta a SAP Commerce en las versiones HY_COM 2105, HY_COM 2205, COM_CLOUD 2211. SAP Commerce Cloud podría permitir que se ingrese una contraseña vacía para la autenticación de ID de usuario y contraseña, lo que habilitaría a los usuarios a acceder al sistema sin necesidad de ingresar una contraseña.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE-1390: Weak Authentication

CVSS Base: **8.8**

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

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

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

Nota	Descripción	Severidad	CVSS
2622660	**Actualización de la Nota de Seguridad publicada en abril de 2018.** Actualizaciones de seguridad para el control del navegador Google Chromium entregadas con SAP Business Client	**Crítica**	10.0
3425274	**CVE-2019-10744**: vulnerabilidad de inyección de código en aplicaciones	**Crítica**	9.4

	construidas con el Producto SAP Build.		
3433192	**CVE-2024-22127**: vulnerabilidad de inyección de código en el producto SAP NetWeaver AS Java (plug-in de visualización de registros de administrador).	**Crítica**	9.1
3346500	**Actualización de la Nota de Seguridad publicada en agosto de 2023.** **CVE-2023-39439**: vulnerabilidad de autenticación incorrecta en el producto SAP Commerce Cloud.	Alta	8.8
3410615	**CVE-2023-44487**: vulnerabilidad de denegación de servicio (DoS) en el producto SAP HANA Database y SAP HANA Extended Application Services Advanced (XS Advanced).	Alta	7.5
3414195	**CVE-2023-50164**: vulnerabilidad de tipo PathTraversing en el producto SAP BusinessObjects Business Intelligence Platform (Central Management Console.	Alta	7.2
3377979	**CVE-2024-27902**: vulnerabilidad de Cross-Site Scripting (XSS) en el producto SAP NetWeaver AS ABAP.	Media	5.4
3425682	**CVE-2024-25644**: vulnerabilidad de divulgación de Información en el producto SAP NetWeaver (WSRM).	Media	5.3
3428847	**CVE-2024-25645**: vulnerabilidad de divulgación de Información en el producto SAP NetWeaver (Enterprise Portal)	Media	5.3
3434192	**CVE-2024-28163**: vulnerabilidad de divulgación de Información en el producto SAP NetWeaver Process Integration (Páginas Web de Soporte).	Media	5.3
3417399	**CVE-2024-22133**: vulnerabilidad de control de acceso inadecuado en el producto SAP Fiori Front End Server.	Media	4.6
3419022	**CVE-2024-27900**: vulnerabilidad de control de acceso inadecuado en el producto SAP Fiori Front End Server.	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 – March 2024.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY