Actualizaciones de seguridad de SAP - Enero 2022

BCSC-ACTUALIZACION-SAP-2022-ENERO

TLP:WHITE

www.basquecybersecurity.eus

Enero 2022

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:

1. RESUMEN EJECUTIVO

SAP ha hecho público el informe de actualizaciones de seguridad de este mes, en donde se aportan soluciones a vulnerabilidades que afectan a varios productos. En total se tratan 9 notas de seguridad en donde la más destacable es la vulnerabilidad Log4j, que afecta a un sistema de registro usado por desarrolladores de aplicaciones web y servidores basados en Java. No se trata de una función que conozcan los usuarios, pero sí una herramienta utilizada por los desarrolladores.

Se recomienda la aplicación de los parches para mantener los sistemas seguros.

2. RECURSOS AFECTADOS

Las actualizaciones de seguridad de este mes están asociados a vulnerabilidades que afectan a los siguientes productos:

- SAP Customer Checkout
- SAP BTP Cloud Foundry
- SAP Landscape Management
- SAP Connected Health Platform 2.0 – Fhirserver
- SAP HANA XS Advanced Cockpit
- SAP NetWeaver Process Integration (Java Web Service Adapter)
- SAP HANA XS Advanced
- Internet of Things Edge Platform
- SAP BTP Kyma
- SAP Enable Now Manager
- SAP Cloud for Customer (add-in for Lotus notes client)
- SAP Localization Hub, digital compliance service for India
- SAP Edge Services On Premise Edition
- SAP Edge Services Cloud Edition
- SAP BTP API Management (Tenant Cloning Tool)
- SAP NetWeaver ABAP Server and ABAP Platform
- SAP Digital Manufacturing Cloud for Edge Computing
- SAP Enterprise Continuous Testing by Tricentis
- SAP Cloud-to-Cloud Interoperability
- Reference Template for enabling ingestion and persistence of time series data in Azure
- SAP Business One
- SAP S/4HANA, Versiones - 100, 101, 102, 103, 104, 105, 106
- SAP NetWeaver AS ABAP - SAP NetWeaver AS ABAP, Versiones - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756
- SAP Business One - SAP Business One, versión - 10
- SAP Enterprise Threat Detection, Versión - 2.0
- SAP NetWeaver AS for ABAP and ABAP Platform, Versions - 701, 702, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 786
- SAP 3D Visual Enterprise Viewer, Versión - 9

- SAP GRC Access Control, Versiones - V1100_700, V1100_731, V1200_750

3. ANÁLISIS TÉCNICO

La lista con todas las vulnerabilidades identificadas se detalla a continuación:

Título	Prioridad	CVSS
[CVE-2021-44228] Nota de seguridad central para la vulnerabilidad de ejecución remota de código asociada con el componente Apache Log4j	**Crítica**	10
[CVE-2022-22531] Múltiples vulnerabilidades en F0743 Crear aplicación de pago único de SAP S/4HANACVE adicional - CVE-2022-22530	Alta	8.7
Actualización de la nota de seguridad publicada el día del parche de diciembre de 2021: [CVE-2021-44235] Vulnerabilidad de inyección de ODA C en la clase de utilidad para SAP NetWeaver AS ABAP	Alta	8.4
[CVE-2021-42066] Vulnerabilidad de divulgación de información en el producto SAP Business One - SAP Business One, versión - 10	Media	6.6
[CVE-2021-44234] Vulnerabilidad de divulgación de información en el producto SAP Business One - SAP Business One, versión - 10	Media	6.5
[CVE-2022-22529] Cross-Site Scripting (XSS) vulnerabilidad en SAP Enterprise Threat Detection	Media	6.1
[CVE-2022-42067] Vulnerabilidad de divulgación de información en SAP NetWeaver Application Server para ABAP y ABAP Platform	Media	4.3
Actualización de la nota de seguridad publicada el día del parche de diciembre de 2021: [CVE-2021-42068,CVE-2021-42070, CVE-2021-42069, CVE-2021-42069] Validación de entrada incorrecta en SAP 3D Visual Enterprise Viewer	Media	4.3
Actualización de la nota de seguridad publicada el día del parche de diciembre de 2021: [CVE-2021-44233] Falta la comprobación de autorización en el control de acceso GRC	Baja	2.4

4. MITIGACIÓN / SOLUCIÓN

SAP publica información sobre los parches que lanza todos los meses en su página web.

5. REFERENCIAS ADICIONALES

- SAP Security Patch Day – January 2022

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?