Actualizaciones de seguridad de SAP - mayo 2022

BCSC-ACTUALIZACIONES-SAP-2022-MAYO

TLP:WHITE

www.basquecybersecurity.eus

Mayo 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

Como todos los meses de forma periódica, SAP ha publicado actualizaciones de seguridad para múltiples productos. Este mes se notifican 10 nuevas notas de seguridad, a las que se añaden 4 actualizaciones de las notas de seguridad publicadas con anterioridad. De todas ellas, 4 tienen carácter crítico, 2 alto y 8 medio.

Desde SAP se sigue poniendo el foco en la vulnerabilidad crítica, de ejecución remota de código en Spring Framework, que se detectó en marzo de 2022 y que se conoce como vulnerabilidad Spring4Shell, con identificador CVE-2022-22965.

Desde el BCSC se recomienda la aplicación de las actualizaciones.

2. RECURSOS AFECTADOS

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

- SAP Business One Cloud, versión 1.1
- SAP Commerce, versiones 1905, 2005, 2105 y 2011
- SAP Customer Profitability Analytics, versión 2
- SAP Webdispatcher, versiones 7.22EXT, 7.49, 7.53, 7.77, 7.81, 7.83, 7.85
- SAP Netweaver AS para ABAP y Java (ICM), versiones KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, 8.04, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 8.04
- Plataforma SAP Business Objects Business Intelligence, versiones 420, 430
- SAP NetWeaver Application Server para plataformas ABAP y ABAP, versiones 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788
- SAP Employee Self Service, versión 605
- SAP NetWeaver Application Server ABAP, versiones 753, 754, 755, 756
- SAP Host Agent, versión 7.22
- SAP NetWeaver y Plataforma ABAP, versiones KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.8
- SAP NetWeaver (ABAP y Java application Servers), versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756
- SAP NetWeaver ABAP Server y plataforma ABAP, versiones 740, 750, 787

3. ANÁLISIS TÉCNICO

Los detalles de la vulnerabilidad crítica corregidas son los siguientes:

CVE-2022-22965: Esta vulnerabilidad afecta a los productos SAP Business One Cloud, SAP Commerce y SAP Customer Profitability Analytics. Una aplicación Spring MVC o Spring WebFlux que se ejecuta en JDK 9+ puede ser vulnerable a la ejecución remota de código a través del enlace de datos. El exploit específico requiere que la aplicación se ejecute en Tomcat como una implementación WAR. Si la aplicación se implementa como un jar ejecutable de Spring Boot, no es vulnerable al exploit. Sin embargo, la naturaleza de la vulnerabilidad es más general y puede haber otras formas de explotarla.

A continuación, se ofrece información sobre las notas de seguridad publicadas:

Nota de seguridad	Severidad	CVSS
3170990 Actualización de la nota de seguridad publicada en abril de 2022 CVE-2022-22965: Nota de seguridad para la vulnerabilidad de ejecución remota de código asociada con Spring Framework	**Crítica**	9.8
3189409 CVE-2022-22965: Vulnerabilidad de ejecución remota de código asociada con Spring Framework utilizada en SAP Business One Cloud	**Crítica**	9.8
3171258 CVE-2022-22965: Vulnerabilidad de ejecución remota de código asociada con Spring Framework utilizada en SAP Commerce	**Crítica**	9.8
3189635 CVE-2022-22965: Vulnerabilidad de ejecución remota de código asociada con Spring Framework utilizada en SAP Customer Profitability Analytics	**Crítica**	9.8
3145046 CVE-2022-27656: Vulnerabilidad de Cross-Site Scripting (XSS) en la interfaz de usuario de administración de SAP Webdispatcher y SAP NetweaverAS para ABAP y Java (ICM)	Alta	8.3
2998510	Alta	7.8

CVE-2022-28214: Vulnerabilidad de divulgación de información del servidor de administración central en la actualización de Business Intelligence		
3137191 Actualización de la nota de seguridad publicada en abril de 2022 CVE-2022-22541: Vulnerabilidad de divulgación de información en la plataforma SAP Business Objects	Media	6.8
3165801 CVE-2022-29611: Vulnerabilidad de falta de comprobación de autorización en la aplicación SAP NetWeaver Server para las plataformas ABAP y ABAP	Media	6.5
3164677 CVE-2022-29613: Vulnerabilidad de divulgación de información en SAP Employee Self Service (Fiori My Leave Request)	Media	6.5
3146336 CVE-2022-29610: Vulnerabilidad de Cross Site Scripting (XSS) en SAP NetWeaver Application Server ABAP	Media	5.4
3158188 CVE-2022-28774: Vulnerabilidad de divulgación de información en el archivo de registro de SAP Host Agent	Media	5.3
3145702 CVE-2022-29616: Vulnerabilidad de daños en la memoria en SAP Host Agent, SAP NetWeaver y plataforma ABAP	Media	5.3
3124994 Actualización de la nota de seguridad publicada en febrero de 2022 CVE-2022-22534: Vulnerabilidad de Cross Site Scripting (XSS) en SAP NetWeaver	Media	4.7
3165333 Actualización de la nota de seguridad publicada en abril de 2022 CVE-2022-28215: Vulnerabilidad de redirección de URL en SAP NetWeaver ABAP Server y plataforma ABAP	Media	4.7

4. MITIGACIÓN / SOLUCIÓN

SAP ha publicado actualizaciones de seguridad y medidas de mitigación para solventar los fallos. La información está disponible en su página web.

5. REFERENCIAS ADICIONALES

- SAP Security Patch Day – May 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?