Actualización fuera de ciclo de Windows Server

BCSC-ACTUALIZACION-WINDOWS-SERVER

TLP:WHITE

www.basquecybersecurity.eus

Noviembre 2021

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 Respuesta 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

Menos de una semana después de la publicación de las actualizaciones correspondientes al mes de noviembre, Microsoft ha lanzado actualizaciones fuera de ciclo para sus versiones de servidor.

Estas actualizaciones, resuelven un problema de autenticación en servidores Windows cuando éstos se usan como controlador de dominio. Según palabras de la propia compañía, "*la autenticación podría fallar en todas las versiones compatibles de Windows Server cuando se usa como controlador de dominio*".

Microsoft también ha asegurado que este fallo estaba causando que los usuarios finales no puedan iniciar sesión en servicios o aplicaciones mediante Single Sign-On.

Las actualizaciones fuera de ciclo de Microsoft no son muy frecuentes, pero desde la compañía se han publicado actualizaciones para solucionar este problema, recomendando a los usuarios la actualización de los dispositivos afectados. Estas actualizaciones se encuentran en el apartado Mitigación / Solución de este mismo documento.

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. ANÁLISIS TÉCNICO

Estas actualizaciones publicadas por Microsoft de una forma excepcional, puesto que se han dado a conocer sólo unos días después de publicar el informe correspondiente al mes de noviembre, abordan un error en varios de sus servidores.

Según Microsoft, el problema reside en la forma en que Windows Server manejaba los tokens de autenticación Kerberos . Específicamente, un error en la extensión *S4u2self* estaba causando que los tickets de Kerberos no se autenticaran correctamente. Este error, como se ha comentado anteriormente, puede provocar que la autenticación falle en los sistemas Windows Server que se utilizan como controlador de dominio. Además, este fallo también puede provocar que los usuarios finales no puedan iniciar sesión en servicios o aplicaciones mediante Single Sign-On.

Este problema afecta a las siguientes versiones de Windows:

- Windows Server 2019.
- Windows Server 2016.
- Windows Server 2012 R2.
- Windows Server 2012.
- Windows Server 2008 R2 SP1.
- Windows Server 2008 SP2.

En adicción a lo anterior, se han hecho públicos por parte de la compañía los errores que se han podido observar en los sistemas afectados:

- El visor de eventos puede mostrar el evento 18 de *Microsoft-Windows-Kerberos-Key-Distribution-Center* registrado en el registro de eventos del sistema.

- Error 0x8009030c. Registro inesperado en el registro de eventos de proxy de aplicación de Azure AD en el evento 12027.

- Los seguimientos de red contienen una firma similar a la siguiente:
  - 7281 24:44 (644) 10.11.2.12.contoso.com KerberosV5 KerberosV5: TGS Request Realm: CONTOSO.COM Sname: http / xxxxx-xxx.contoso.com

  - 7282 7290 (0). CONTOSO.COM.

3. MITIGACIÓN / SOLUCIÓN

Microsoft ha publicado correcciones para esta vulnerabilidad, por lo que se recomienda aplicar las actualizaciones correspondientes:

- Windows Server 2019: KB5008602.
- Windows Server 2016: KB5008601.
- Windows Server 2012 R2: KB5008603.
- Windows Server 2012: KB5008604.
- Windows Server 2008 R2 SP1: KB5008605.
- Windows Server 2008 SP2: KB5008606.

Destacar que estas actualizaciones no se pueden aplicar a través de Windows Update, por lo tanto, se deben usar los enlaces indicados anteriormente, o en su defecto, buscar la actualización correspondiente en el catálogo de actualizaciones de Microsoft y seguir las instrucciones indicadas.

Por último, señalar que debido a que el error solo afecta a sistemas Windows Server que se utilizan como controlador de dominio, no será necesario actualizar los equipos de los usuarios finales que ejecutan la versión cliente de Windows.

4. REFERENCIAS ADICIONALES

- New Microsoft emergency updates fix Windows Server auth issues.
- Microsoft rolled out emergency updates to fix Windows Server auth failures.
- Actualización KB5008601.
- Actualización KB5008602.
- Actualización KB5008603.
- Actualización KB5008604.
- Actualización KB5008605.
- Actualización KB5008606.
- WSUS and the Catalog Site.
- Kerberos Authentication Overview.
- What is single sign-on in Azure Active Directory?

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?