Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Vulnerabilidad en escalada de privilegios en AD

14/mayo/2022

Contenido

Introducción

Con este boletín, le presentamos información muy importante sobre una vulnerabilidad que permite a los actores de amenazas obtener escalada de privilegios dentro de su servidor de dominio.

PARCHES PARA VULNERABILIDAD ENCONTRADA EN AD.

A continuación, se encuentra en cuadro de identificación de la vulnerabilidad.

ID de alerta:	DSOC-CERT_2022_05_14
Clasificación de alerta:	VULNERABILIDAD
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/14/2022
Es día cero (0 day):	NO

RESUMEN

Los ataques de explotación de privilegios en los entornos de dominio de Windows Active Directory (AD) de Microsoft están ampliando su alcance y creciendo en escala para apuntar a millones de dispositivos. El Centro de respuestas de seguridad de Microsoft (MSRC) actualizó recientemente la información sobre fallas de seguridad que afectan los productos y servicios de la compañía, destacando la vulnerabilidad de elevación de privilegios de los Servicios de dominio de Active Directory recientemente descubierta y rastreada como CVE-2022–26923 .

La falla de escalada de privilegios de dominio de Active Directory recientemente revelada aún no se ha explotado en la naturaleza, aún tiene un alto 8.8. La puntuación de CVSS apunta a un alto riesgo que representa para los sistemas comprometidos, lo que permite a los atacantes abusar de los problemas del certificado. CVE-2022–26923 permite manipular el atributo DnsHostName, que especifica el nombre de la computadora tal como está registrado en DNS, y luego permite que un adversario obtenga un certificado de los Servicios de certificados de AD, lo que podría generar una elevación de privilegios.

Para las medidas de protección y mitigación CVE-2022-26923, Microsoft recomienda encarecidamente actualizar todos los servidores que ejecutan los servicios de certificados de AD y los controladores de dominio de Windows que operan la autenticación basada en certificados a la última versión del 10 de mayo.

RECOMENDACIONES

Se recomiendan las siguientes acciones:

- Programar una ventana de mantenimiento para aplicar las actualizaciones.
- Prestar atención a las alertas de su SOC sobre conexiones y firmas sospechosas.
- Asegúrese que sus equipos perimetrales se encuentren en una versión de firmware reciente.
- Siempre estar alerta ante las noticias de este tipo para poder mitigar vulnerabilidades antes de que un actor malicioso pueda explotarlas.

ENLACES DE DESCARGA

Vulnerabilidad de elevación de privilegios de los servicios de dominio de Active Directory

Product	Download
Windows Server 2012 R2 (Server Core installation)	Monthly Rollup
Windows Server 2012 R2 (Server Core installation)	Security Only
Windows Server 2012 R2	Monthly Rollup
Windows Server 2012 R2	Security Only
Windows RT 8.1	ServicingStackUpdate
Windows 8.1 for x64-based systems	Monthly Rollup
Windows 8.1 for x64-based systems	Security Only
Windows 8.1 for 32-bit systems	Monthly Rollup
Windows 8.1 for 32-bit systems	Security Only
Windows Server 2016 (Server Core installation)	Security Update
Windows Server 2016	Security Update
Windows 10 Version 1607 for x64-based Systems	Security Update
Windows 10 Version 1607 for 32-bit Systems	Security Update
Windows 10 for x64-based Systems	Security Update
Windows 10 for 32-bit Systems	Security Update
Windows 10 Version 21H2 for x64-based Systems	Security Update
Windows 10 Version 21H2 for ARM64-based Systems	Security Update
Windows 10 Version 21H2 for 32-bit Systems	Security Update
Windows 11 for ARM64-based Systems	Security Update
Windows 11 for x64-based Systems	Security Update
Windows Server, version 20H2 (Server Core Installation)	Security Update
Windows 10 Version 20H2 for ARM64-based Systems	Security Update
Windows 10 Version 20H2 for 32-bit Systems	Security Update
Windows 10 Version 20H2 for x64-based Systems	Security Update
Windows Server 2022 (Server Core installation)	Security Update
Windows Server 2022	Security Update
Windows 10 Version 21H1 for 32-bit Systems	Security Update
Windows 10 Version 21H1 for ARM64-based Systems	Security Update
Windows 10 Version 21H1 for x64-based Systems	Security Update
Windows 10 Version 1909 for ARM64-based Systems	Security Update
Windows 10 Version 1909 for x64-based Systems	Security Update
Windows 10 Version 1909 for 32-bit Systems	Security Update
Windows Server 2019 (Server Core installation)	Security Update
Windows Server 2019	Security Update
Windows 10 Version 1809 for ARM64-based Systems	Security Update
Windows 10 Version 1809 for x64-based Systems	Security Update
Windows 10 Version 1809 for 32-bit Systems	Security Update

Noticia Completa

https://socprime.com/blog/cve-2022-26923-detection-active-directory-domain-privilege-escalation-vulnerability/

https://research.ifcr.dk/certifried-active-directory-domain-privilege-escalation-cve-2022-26923-9e098fe298f4

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente