Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Amenazas de día cero

.

11/mayo/2022

Contenido

Introducción 3

Parches para amenazas de día cero. 4

Resumen 4

Recomendaciones.....6

Enlaces de descarga.....7

Noticia Completa 8

Contactos de soporte 9

INTRODUCCIÓN

Con este boletín, le presentamos información relevante sobre amenazas de día cero encontradas recientemente, por favor revisar detenidamente el documento para validar que sus plataformas no se vean afectadas por estos hallazgos.

PARCHES PARA AMENAZAS DE DÍA CERO.

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

ID de alerta:	DSOC-CERT_2022_05_11
Clasificación de alerta:	VULNERABILIDAD
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/10/2022
Es día cero (0 day):	SI

RESUMEN

El día 10 de mayo se han liberado actualizaciones que corrigen fallas de día cero en las siguientes plataformas:

1. Redshift ODBC Driver
2. Windows LSA Spoofing Vulnerability
3. Windows Hyper-V Denial of Service Vulnerability

Vectores de ataque:

En el caso de la vulnerabilidad en RedShift, la explotación de esta vulnerabilidad requiere que un atacante tenga al menos uno de los siguientes roles:

Administrador de sinapsis
Colaborador de sinapsis
Operador de cómputo Synapse

En Windows LSA Spoofing Vulnerability, Un atacante no autenticado podría llamar a un método en la interfaz LSARPC y obligar al controlador de dominio a autenticarse ante el atacante mediante NTLM. Se recomienda aplicar el parche, ya que esta actualización de seguridad detecta intentos de conexión anónimos en LSARPC y los rechaza.

Con la denegación de servicios de Hyper-V, el atacante debe ganar una "condición de carrera" para poder a cabo su actividad maliciosa.

RECOMENDACIONES

Se recomiendan las siguientes acciones:

- Programar a la brevedad 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.

ENLACES DE DESCARGA

Windows LSA Spoofing Vulnerability

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 Server 2012 (Server Core installation)	Monthly Rollup
Windows Server 2012 (Server Core installation)	Security Only
Windows Server 2012	Monthly Rollup
Windows Server 2012	Security Only
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Monthly Rollup
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Security Only
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Monthly Rollup
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Security Only
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Monthly Rollup
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Security Only
Windows Server 2008 for x64-based Systems Service Pack 2	Monthly Rollup
Windows Server 2008 for x64-based Systems Service Pack 2	Security Only
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Monthly Rollup
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Security Only
Windows Server 2008 for 32-bit Systems Service Pack 2	Monthly Rollup
Windows Server 2008 for 32-bit Systems Service Pack 2	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 7 for x64-based Systems Service Pack 1	Monthly Rollup
Windows 7 for x64-based Systems Service Pack 1	Security Only
Windows 7 for 32-bit Systems Service Pack 1	Monthly Rollup
Windows 7 for 32-bit Systems Service Pack 1	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

Windows Hyper-V Denial of Service Vulnerability

Product	Download
Windows 10 Version 21H2 for x64-based Systems	Security Update
Windows Server, version 20H2 (Server Core Installation)	Security Update
Windows 10 Version 20H2 for x64-based Systems	Security Update
Windows 10 Version 21H1 for x64-based Systems	Security Update

Redshift ODBC Driver

Product	Download
Self-hosted Integration Runtime	Security Update

Noticia Completa

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26925

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22713

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