Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Microsoft emite parches para 6 día cero explotados activamente.

09/Noviembre/2022

Contenido

Introducción

La última ronda de actualizaciones de seguridad mensuales de Microsoft se lanzó con correcciones para 68 vulnerabilidades que abarcan su cartera de software, incluidos parches para seis días cero explotados activamente.

MICROSOFT CORRIGE MÚLTIPLES VULNERABILIDADES

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

ID de alerta:	DSOC-CERT_2022_11_09_1
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/09/2022
Es día cero (0 day):	Si

RESUMEN

12 de los problemas se califican como Críticos, dos como Altos y 55 como Importantes en gravedad. Esto también incluye las debilidades que fueron cerradas por OpenSSL la semana anterior.

También se abordó por separado a principios de mes una falla explotada activamente en los navegadores basados en Chromium (CVE-2022-3723) que Google tapó como parte de una actualización fuera de banda a fines del mes pasado.

La gran noticia es que dos CVE de día cero anteriores que afectaban a Exchange Server, que se hicieron públicos a fines de septiembre, finalmente se solucionaron", dijo Greg Wiseman, gerente de producto de Rapid7.

Se recomienda a los clientes que actualicen sus sistemas de Exchange Server de inmediato, independientemente de si se han aplicado los pasos de mitigación recomendados anteriormente. Las reglas de mitigación ya no se recomiendan una vez que se han parcheado los sistemas.

La lista de vulnerabilidades explotadas activamente, que permiten la elevación de privilegios y la ejecución remota de código, es la siguiente:

CVE-2022-41040 (puntuación CVSS: 8,8): vulnerabilidad de elevación de privilegios de Microsoft Exchange Server (también conocido como ProxyNotShell)

CVE-2022-41082 (puntuación CVSS: 8,8): vulnerabilidad de elevación de privilegios de Microsoft Exchange Server (también conocido como ProxyNotShell)

CVE-2022-41128 (puntuación CVSS: 8,8): vulnerabilidad de ejecución remota de código de lenguajes de secuencias de comandos de Windows

CVE-2022-41125 (puntuación CVSS: 7,8): vulnerabilidad de elevación de privilegios del servicio de aislamiento de claves CNG de Windows

CVE-2022-41073 (puntuación CVSS: 7,8): vulnerabilidad de elevación de privilegios de la cola de impresión de Windows

CVE-2022-41091 (puntuación CVSS: 5,4): marca de Windows de la vulnerabilidad de omisión de la función de seguridad web

A Benoît Sevens y Clément Lecigne del Threat Analysis Group (TAG) de Google se les atribuye el informe CVE-2022-41128, que reside en el componente JScript9 y ocurre cuando se engaña a un objetivo para que visite un sitio web especialmente diseñado.

CVE-2022-41091 es una de las dos fallas de omisión de seguridad en Windows Mark of the Web (MoTW) que salió a la luz en los últimos meses. Recientemente fue descubierto como arma por el actor de ransomware Magniber para apuntar a los usuarios con actualizaciones de software falsas.

"Un atacante puede crear un archivo malicioso que evadiría las defensas de Mark of the Web (MotW), lo que resultaría en una pérdida limitada de integridad y disponibilidad de funciones de seguridad como Vista protegida en Microsoft Office, que se basan en el etiquetado de MotW", dijo Microsoft en un aviso

La segunda falla de MotW que se resolverá es CVE-2022-41049 (también conocida como ZippyReads). Informado por el investigador de seguridad de Analygence, Will Dormann, se relaciona con una falla al establecer el indicador Mark of the Web en los archivos de almacenamiento extraídos.

Es probable que los actores de amenazas abusen de las dos fallas de escalada de privilegios en Print Spooler y CNG Key Isolation Service como seguimiento de un compromiso inicial y obtengan privilegios de SISTEMA, dijo Kev Breen, director de investigación de amenazas cibernéticas en Immersive Labs.

"Se requiere este nivel más alto de acceso para deshabilitar o alterar las herramientas de monitoreo de seguridad antes de ejecutar ataques de credenciales con herramientas como Mimikatz que pueden permitir a los atacantes moverse lateralmente a través de una red", agregó Breen.

Otras cuatro vulnerabilidades calificadas como críticas en el parche de noviembre que vale la pena señalar son fallas de elevación de privilegios en Windows Kerberos (CVE-2022-37967), Kerberos RC4-HMAC (CVE-2022-37966) y Microsoft Exchange Server (CVE-2022-41080).) y una falla de denegación de servicio que afecta a Windows Hyper-V (CVE-2022-38015).

La lista de correcciones para fallas críticas se completa con cuatro vulnerabilidades de ejecución remota de código en el Protocolo de túnel punto a punto (PPTP), todas con puntajes CVSS de 8.1 (CVE-2022-41039 , CVE-2022-41088 y CVE- 2022-41044), y otro impactante lenguaje de secuencias de comandos de Windows JScript9 y Chakra (CVE-2022-41118).

Además de estos problemas, la actualización de Patch Tuesday también resuelve una serie de fallas de ejecución remota de código en Microsoft Excel, Word, ODBC Driver, Office Graphics, SharePoint Server y Visual Studio, así como una serie de errores de escalada de privilegios en Win32k, Filtro superpuesto y directiva de grupo.

PARCHES DE SOFTWARE DE OTROS PROVEEDORES

Aparte de Microsoft, otros proveedores también han lanzado actualizaciones de seguridad desde principios de mes para rectificar varias vulnerabilidades, que incluyen:

AMD
Android
Apple
Cisco
Citrix
CODESYS
Dell
F5
Fortinet
GitLab
Google Chrome
HP
IBM
Intel
Juniper Networks
Linux distributions Debian, Oracle Linux, Red Hat, SUSE, and Ubuntu
MediaTek
NVIDIA
Qualcomm
SAP
Schneider Electric
Siemens
Trend Micro
VMware
WordPress

Actualizaciones de seguridad del martes de parches de noviembre de 2022

A continuación, se muestra la lista completa de vulnerabilidades resueltas y avisos publicados en las actualizaciones del martes de parches de noviembre de 2022. Para acceder a la descripción completa de cada vulnerabilidad y los sistemas a los que afecta. Puede visualizar el reporte aquí.

Recomendaciones

- Se recomienda instalar las actualizaciones en todos sus equipos rápidamente.

- Validar que todas sus herramientas y dispositivos de seguridad cuenten con las versiones de firmware más recientes.

- Mantener monitoreo sobre posibles futuras amenazas para aplicar correcciones y así evitar su explotación.

Noticia Completa

https://devel.group/blog/parches-emitidos-para-6-dias-cero-explotados-activamente/

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