Microsoft ha lanzado actualizaciones para solucionar un total de 143 fallos de seguridad como parte de sus actualizaciones de seguridad mensuales, dos de los cuales han sido explotados activamente en la naturaleza.

Cinco de los 143 fallos están clasificados como Críticos, 136 como Importantes y cuatro como Moderados en cuanto a severidad. Estas correcciones se suman a las 33 vulnerabilidades que se han abordado en el navegador Edge basado en Chromium durante el último mes.

Los dos fallos de seguridad que han sido explotados son los siguientes:

- CVE-2024-38080 (puntuación CVSS: 7.8): Vulnerabilidad de elevación de privilegios en Windows Hyper-V.
- CVE-2024-38112 (puntuación CVSS: 7.5): Vulnerabilidad de suplantación de la plataforma MSHTML de Windows.

> *«La explotación exitosa de esta vulnerabilidad requiere que un atacante tome acciones adicionales antes de la explotación para preparar el entorno objetivo. Un atacante tendría que enviar a la víctima un archivo malicioso que la víctima tendría que ejecutar»*, explicó Microsoft sobre la CVE-2024-38112.

Haifei Li, investigador de seguridad de Check Point, quien ha sido acreditado con el descubrimiento y la denuncia de la falla en mayo de 2024, indicó que los actores de amenazas están utilizando archivos de acceso directo de Internet de Windows (.URL) especialmente diseñados que, al hacer clic, redirigen a las víctimas a una URL maliciosa invocando el navegador retirado Internet Explorer (IE).

> *«Se emplea un truco adicional en IE para ocultar el nombre de la extensión maliciosa .HTA. Al abrir la URL con IE en lugar de los navegadores modernos y mucho más seguros Chrome/Edge en Windows, el atacante obtuvo ventajas significativas en la explotación de la computadora de la víctima, aunque la*

> *computadora esté ejecutando el sistema operativo moderno Windows 10/11»,* explicó Li.
>
> *«CVE-2024-38080 es una falla de elevación de privilegios en Windows Hyper-V. Un atacante local, autenticado, podría explotar esta vulnerabilidad para elevar privilegios al nivel de SISTEMA tras una primera compromisión de un sistema objetivo»,* dijo Satnam Narang, ingeniero de investigación sénior en Tenable.

Aunque los detalles exactos sobre el abuso de la CVE-2024-38080 son actualmente desconocidos, Narang señaló que esta es la primera de las 44 fallas de Hyper-V que se explota en la naturaleza desde 2022.

Otras dos fallas de seguridad corregidas por Microsoft han sido catalogadas como públicamente conocidas en el momento del lanzamiento. Esto incluye un ataque de canal lateral llamado FetchBench (CVE-2024-37985, puntuación CVSS: 5.9) que podría permitir a un adversario ver la memoria heap de un proceso privilegiado que se ejecuta en sistemas basados en ARM.

La segunda vulnerabilidad divulgada públicamente es CVE-2024-35264 (puntuación CVSS: 8.1), un error de ejecución remota de código que afecta a .NET y Visual Studio.

> *«Un atacante podría explotar esto cerrando una secuencia http/3 mientras se procesa el cuerpo de la solicitud, lo que lleva a una condición de carrera. Esto podría resultar en la ejecución remota de código»*, dijo Redmond en un aviso.

También se resolvieron como parte de las actualizaciones de Patch Tuesday 37 fallas de ejecución remota de código que afectan al Proveedor OLE DB del Cliente Nativo de SQL Server, 20 vulnerabilidades de omisión de la característica de seguridad Secure Boot, tres errores de escalada de privilegios de PowerShell y una vulnerabilidad de suplantación en el

protocolo RADIUS (CVE-2024-3596, también conocido como BlastRADIUS).

> *«[Las fallas de SQL Server] afectan específicamente al Proveedor OLE DB, por lo que no solo se deben actualizar las instancias de SQL Server, sino que también se debe abordar el código cliente que ejecuta versiones vulnerables del controlador de conexión»,* dijo Greg Wiseman, Gerente de Producto Líder de Rapid7.
>
> *«Por ejemplo, un atacante podría usar tácticas de ingeniería social para engañar a un usuario autenticado para que intente conectarse a una base de datos de SQL Server configurada para devolver datos maliciosos, permitiendo la ejecución arbitraria de código en el cliente».*

Para concluir la larga lista de parches está CVE-2024-38021 (puntuación CVSS: 8.8), una falla de ejecución remota de código en Microsoft Office que, si se explota con éxito, podría permitir a un atacante obtener altos privilegios, incluyendo la capacidad de leer, escribir y eliminar.

Morphisec, que reportó la falla a Microsoft a finales de abril de 2024, dijo que la vulnerabilidad no requiere ninguna autenticación y representa un riesgo grave debido a su naturaleza de cero clics.

> *«Los atacantes podrían explotar esta vulnerabilidad para obtener acceso no autorizado, ejecutar código arbitrario y causar daños sustanciales sin ninguna interacción del usuario. La ausencia de requisitos de autenticación la hace particularmente peligrosa, ya que abre la puerta a una explotación generalizada»,* dijo Michael Gorelik.

Las correcciones se producen después de que Microsoft anunciara a finales del mes pasado

que comenzará a emitir identificadores CVE para vulnerabilidades de seguridad relacionadas con la nube en adelante, en un intento por mejorar la transparencia.

Parches de software de otros proveedores

Además de Microsoft, otros proveedores también han lanzado actualizaciones de seguridad en las últimas semanas para corregir varias vulnerabilidades, incluyendo:

- Adobe
- Amazon Web Services
- AMD
- Apple
- Arm
- Broadcom (incluyendo VMware)
- Cisco
- Citrix
- CODESYS
- D-Link
- Dell
- Drupal
- Emerson
- F5
- Fortinet
- Fortra FileCatalyst Workflow
- GitLab
- Google Android
- Google Chrome
- Google Cloud
- Google Pixel
- Google Wear OS
- Hitachi Energy
- HP

- HP Enterprise
- IBM
- Ivanti
- Jenkins
- Juniper Networks
- Lenovo
- Distribuciones Linux: Amazon Linux, Debian, Oracle Linux, Red Hat, Rocky Linux, SUSE y Ubuntu
- MediaTek
- Mitsubishi Electric
- MongoDB
- Mozilla Firefox y Firefox ESR
- NETGEAR
- NVIDIA
- OpenSSH
- Progress Software
- QNAP
- Qualcomm
- Rockwell Automation
- Samsung
- SAP
- Schneider Electric
- Siemens
- Splunk
- Spring Framework
- TP-Link
- Veritas
- WordPress
- Zoom