Microsoft ha publicado actualizaciones de seguridad para corregir un total de 118 vulnerabilidades en sus productos de software, dos de las cuales ya están siendo activamente explotadas en el entorno real.

De esas 118 fallas, tres han sido calificadas como críticas, 113 como importantes y dos como de severidad moderada. La actualización de seguridad de este martes no incluye 25 vulnerabilidades adicionales que la compañía abordó en su navegador Edge basado en Chromium durante el mes pasado.

Cinco de las vulnerabilidades eran de conocimiento público en el momento de su lanzamiento, y dos de ellas están siendo explotadas activamente como fallas de día cero:

- CVE-2024-43572 (Puntuación CVSS: 7.8) – Vulnerabilidad de ejecución de código remoto en Microsoft Management Console (se detectó explotación).
- CVE-2024-43573 (Puntuación CVSS: 6.5) – Vulnerabilidad de suplantación en la plataforma MSHTML de Windows (se detectó explotación).
- CVE-2024-43583 (Puntuación CVSS: 7.8) – Vulnerabilidad de escalada de privilegios en Winlogon.
- CVE-2024-20659 (Puntuación CVSS: 7.1) – Vulnerabilidad de omisión de funciones de seguridad en Windows Hyper-V.
- CVE-2024-6197 (Puntuación CVSS: 8.8) – Vulnerabilidad de ejecución de código remoto en Curl de código abierto (vulnerabilidad no relacionada con Microsoft).

Es relevante destacar que CVE-2024-43573 es similar a CVE-2024-38112 y CVE-2024-43461, otras vulnerabilidades de suplantación en MSHTML que fueron previamente explotadas por el grupo de amenazas *Void Banshee* para distribuir el malware *Atlantida Stealer* antes de julio de 2024.

Microsoft no ha proporcionado detalles sobre cómo se están explotando estas dos vulnerabilidades o quién está detrás de los ataques, ni la magnitud de los mismos. La empresa reconoció a los investigadores Andres y Shady por informar sobre CVE-2024-43572, pero no ofreció crédito por CVE-2024-43573, lo que sugiere que podría tratarse de un caso de

elusión de parche.

> *«Desde el descubrimiento de CVE-2024-43572, Microsoft ha bloqueado la apertura de archivos MSC no confiables en un sistema»,* declaró Satnam Narang, ingeniero de investigación senior en Tenable.

La Agencia de Seguridad Cibernética y de Infraestructura de los EE. UU. (CISA) también mencionó la explotación activa de CVE-2024-43572 y CVE-2024-43573, incluyéndolas en su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) y requiriendo a las agencias federales implementar las correcciones antes del 29 de octubre de 2024.

Entre todas las fallas reveladas por Microsoft en esta actualización, la más grave es una vulnerabilidad de ejecución remota de código en Microsoft Configuration Manager (CVE-2024-43468, puntuación CVSS: 9.8) que permitiría a atacantes no autenticados ejecutar comandos arbitrarios.

> *«Un atacante sin autenticación podría explotar esta vulnerabilidad enviando solicitudes especialmente diseñadas al entorno objetivo, las cuales son procesadas de forma insegura, lo que permite al atacante ejecutar comandos en el servidor o en la base de datos subyacente»,* se explicó.

Dos vulnerabilidades críticas adicionales también están relacionadas con la ejecución remota de código, una en la extensión de Visual Studio Code para Arduino (CVE-2024-43488, puntuación CVSS: 8.8) y otra en el servidor del Protocolo de Escritorio Remoto (RDP) (CVE-2024-43582, puntuación CVSS: 8.1).

> *«La explotación requiere que el atacante envíe paquetes malformados a un host RPC de Windows, lo que resulta en la ejecución de código en el contexto del servicio*

> *RPC. Sin embargo, lo que esto implica en la práctica puede depender de la configuración de la restricción de la interfaz RPC en el sistema objetivo»,* explicó Adam Barnett, ingeniero líder de software en Rapid7, sobre CVE-2024-43582.
>
> *«Un aspecto positivo es que la complejidad del ataque es alta, ya que el atacante debe superar una condición de carrera para acceder a la memoria de manera incorrecta».*