Microsoft corrigió hasta 121 nuevas vulnerabilidades de seguridad como parte de sus actualizaciones de Patch Tuesday para el mes de agosto, que también incluye una corrección para una vulnerabilidad de la herramienta de diagnóstico de soporte que, según la compañía, se está explotando activamente en la naturaleza.

De los 121 errores, 17 se califican como Críticos, 102 como importantes, uno como moderado y otro como bajo en nivel de gravedad. De los problemas se enumeraron como conocidos públicamente en el momento del lanzamiento.

Cabe mencionar que las 121 vulnerabilidades se suman a las 25 deficiencias que la compañía abordó en su navegador web Edge basado en Chromium a fines del mes pasado y la semana anterior.

Encabezando la lista de parches se encuentra CVE-2022-34713 (puntuación CVSS: 7.8), un caso de ejecución remota de código que afecta a la herramienta de diagnóstico de soporte de Microsoft Windows (MSDT), lo que la convierte en la segunda falla en el mismo componente de Follina (CVE-2022-30190) para ser armado en ataques del mundo real dentro de tres meses.

También se cree que la vulnerabilidad es una variante de la falla conocida públicamente como DogWalk, que fue revelada originalmente por el investigador de seguridad Imre Rad en enero de 2020.

> *«La explotación de la vulnerabilidad requiere que un usuario abra un archivo especialmente diseñado. En un escenario de ataque por correo electrónico, un atacante podría explotar la vulnerabilidad enviando el archivo especialmente diseñado al usuario y convencerlo de que abra el archivo»,* dijo Microsoft.

Alternativamente, un atacante podría alojar un sitio web o aprovechar un sitio ya comprometido que contiene un archivo con malware diseñado para explotar la vulnerabilidad y después engañar a los objetivos potenciales para que hagan clic en un enlace en un correo

electrónico o un mensaje instantáneo para abrir el documento.

> *«Este no es un vector poco común y los documentos y enlaces maliciosos todavía son utilizados por los atacantes con gran efecto. Subraya la necesidad de mejorar las habilidades de los empleados para que desconfíen de dichos ataques»,* dijo Kev Breen, director de investigación de amenazas cibernéticas en Immersive Labs.

CVE-2022-34713 es una de las dos vulnerabilidades de ejecución remota de código en MSDT cerrada por Redmond este mes, la otra es CVE-2022-35743 (puntaje CVSS: 7.8). A los investigadores de seguridad Bill Demirkapi y Matt Braeber se les atribuye haber informado sobre la vulnerabilidad.

Microsoft también resolvió tres fallas de escalada de privilegios en Exchange Server que podrían usarse para leer mensajes de correo electrónico específicos y descargar archivos adjuntos (CVE-2022-21980, CVE-2022-24477 y CVE-2022-24516) y una vulnerabilidad de divulgación de información conocida públicamente (CVE-2022-30134) en Exchange, lo que también podría generar el mismo impacto.

> *«Los administradores deben habilitar la protección extendida para remediar completamente esta vulnerabilidad»,* dijo Greg Wiseman, gerente de producto de Rapid7, acerca de CVE-2022-30134.

La actualización de seguridad corrige aún más múltiples vulnerabilidades de ejecución remota de código en el Protocolo Punto a Punto (PPP) de Windows, el Protocolo de Túnel de Sockets Seguros (SSTP) de Windows, Azure RTOS GUIX Studio, Microsoft Office y Windows Hyper-V.

La corrección del martes de parches también se destaca por abordar docenas de vulnerabilidades de escalada de privilegios: 31 en Azure Site Recovery, un mes después de

que Microsoft eliminó 30 errores similares en el servicio de continuidad comercial, cinco en Storage Spaces Direct, tres en Windows Kernel y dos en el Módulo de Cola de Impresión.

Parches de software de otros proveedores

Además de Microsoft, otros proveedores también lanzaron actualizaciones de seguridad desde inicios del mes para corregir varias vulnerabilidades, incluyendo:

- Adobe
- AMD
- Android
- Apache Projects
- Cisco
- Citrix
- Dell
- F5
- Fortinet
- GitLab
- Google Chrome
- HP
- IBM
- Intel
- Distribuciones de Linux Debian, Oracle Linux, Red Hat, SUSE y Ubuntu
- MediaTek
- NVIDIA
- Qualcomm
- Samba
- SAVIA
- Schneider Electric
- Siemens
- VMware