Microsoft lanzó este martes parches de seguridad para contener un total de 71 vulnerabilidades en Microsoft Windows y otro software, incluyendo una solución para una vulnerabilidad de escalada de privilegios explotada activamente que podría explotarse junto con errores de ejecución remota de código para tomar el control de los sistemas vulnerables.

Dos de las vulnerabilidades abordadas se clasifican como críticas, 68 se clasifican como importantes y una tiene gravedad baja, y tres de los problemas se enumeran como de conocimiento público en el momento del lanzamiento. Los cuatro días cero son los siguientes:

- CVE-2021-40449 (puntuación CVSS: 7.8): Vulnerabilidad de elevación de privilegios de Win32K
- CVE-2021-41335 (puntuación CVSS: 7.8): Vulnerabilidad de elevación de privilegios del kernel de Windows
- CVE-2021-40469 (puntuación CVSS: 7.2): Vulnerabilidad de ejecución remota de código del servidor DNS de Windows
- CVE-2021-41338 (puntuación CVSS: 5.5): Vulnerabilidad de omisión de la función de seguridad de las reglas de firewall de Windows AppContainter

La vulnerabilidad rastreada como CVE-2021-40449, se refiere a una falla de uso después de la liberación en el controlador del kernel Win32k que Kaspersky descubrió como explotada en la naturaleza a fines de agosto y principios de septiembre de 2021, como parte de una campaña de espionaje generalizada dirigida a empresas de TI, contratistas de defensa y entidades diplomáticas. La compañía rusa de ciberseguridad denominó al grupo de amenazas como «*MysterySnail*«.

> *«La similitud de código y la reutilización de la infraestructura C2 que descubrimos nos permitió conectar estos ataques con el actor conocido como IronHusky, y la actividad APT de habla china que se remonta a 2012»*, informaron los investigadores de Kaspersky, Boris Larin y Costin Raiu.

En el informe técnico de los investigadores, se detalla que las cadenas de infección conducen

al despliegue de un troyano de acceso remoto capaz de recopilar y extraer información del sistema de los hosts comprometidos antes de comunicarse con su servidor C2 para obtener más instrucciones.

Otras vulnerabilidades notables incluyen fallas de ejecución remota de código que afectan a Microsoft Exchange Server (CVE-2021-26427), Windows Hyper-V (CVE-2021-38672 y CVE-2021-40461), SharePoint Server (CVE-2021-40487 y CVE-2021-41344) y Microsoft Word (CVE-2021-40486), así como una falla en la divulgación de información en el control de edición de texto enriquecido (CVE-2021-40454).

CVE-2021-26427, que tiene una puntuación CVSS de 9.0 y fue identificado por la Agencia de Seguridad Nacional de Estados Unidos, subraya que *«los servidores Exchange son objetivos de alto valor para los hackers que buscan penetrar en las redes comerciales»*, dijo Bharat Jogi, gerente senior de vulnerabilidad e investigación de amenazas en Qualys.

El martes de parches de octubre se completa con correcciones para dos deficiencias recientemente descubiertas en el componente de cola de impresión, CVE-2021-41332 y CVE-2021-36970, cada una relacionada con un error de divulgación de información y una vulnerabilidad de suplantación de identidad, que se ha etiquetado como *«explotación más probable»* en la evaluación del índice de explotabilidad.

> *«Una vulnerabilidad de suplantación de identidad generalmente indica que un atacante puede suplantar o identificarse como otro usuario. En este caso, parece que un atacante puede abusar del servicio Spooler para cargar archivos arbitrarios a otros servidores»*, dijo el investigador de seguridad Ollypwn en Twitter.