La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó esta semana 95 vulnerabilidades de seguridad a su Catálogo de Vulnerabilidades Explotadas Conocidas, elevando el número total de vulnerabilidades explotadas activamente a 478.

> *«Este tipo de vulnerabilidades son un vector de ataque frecuente para los ciberdelincuentes maliciosos y representan un riesgo significativo para la empresa federal»,* dijo la agencia en un aviso del 3 de marzo de 2022.

De los 95 errores agregados recientemente, 38 se relacionan con vulnerabilidades de Cisco, 27 para Microsoft, 16 para Adobe, 7 afectan a Oracle y uno corresponde a Apache Tomcat, ChakraCore, Exim, Mozilla Firefox, Linux Kernel, Siemens SIMANTIC CP y Treck TCP/IP Stack.

En la lista se incluyen cinco problemas descubiertos en los enrutadores Cisco RV, que CISA asegura se están explotando en ataques del mundo real. Las vulnerabilidades, que salieron a la luz a inicios del mes pasado, permiten la ejecución remota de código arbitrario con privilegios de root.

Tres de las vulnerabilidades, CVE-2022-20699, CVE-2022-20700 y CVE-2022-20708, tienen una calificación de 10 sobre 10 en la escala de calificación CVSS, lo que permite a un atacante inyectar comandos maliciosos, elevar los privilegios a raíz y ejecutar código arbitrario en sistemas vulnerables.

CVE-2022-20701 (puntuación CVSS de 9.0) y CVE-2022-20703 (puntuación CVSS de 9.3) no son diferentes en el sentido de que podrían permitir que un adversario *«ejecute código arbitrario, eleve los privilegios, ejecute comandos arbitrarios, omita las protecciones de autenticación y autorización, buscar y ejecutar software sin firmar, o causar una denegación de servicio»,* dijo CISA.

Por su parte, Cisco reconoció previamente que está *«consciente de que el código de explotación de prueba de concepto está disponible para varias de las vulnerabilidades».* Aún

se desconoce la naturaleza adicional de los ataques o los actores de amenazas que pueden estar usándolos como armas.

Para reducir el riesgo significativo de las vulnerabilidades y evitar que se utilicen como vector de posibles ataques cibernéticos, las agencias federales de Estados Unidos tienen la obligación de aplicar los parches antes del 17 de marzo de 2022.

El desarrollo se produce poco después de que Cisco lanzara parches para vulnerabilidades de seguridad críticas que afectan a Expressway Series y Cisco TelePresence Video Communication Server (VCS) esta semana, que podrían ser explotadas para obtener privilegios elevados y ejecutar código arbitrario.