Cisco advirtió sobre intentos de explotación activos dirigidos a un par de vulnerabilidades de seguridad de dos años en Cisco AnyConnect Secure Mobility Client para Windows.

Rastreadas como CVE-2020-3153 (puntuación CVSS: 6.5) y CVE-2020-3433 (puntuación CVSS: 7.8), las vulnerabilidades podrían permitir a los hackers autenticados locales secuestrar DLL y copiar archivos arbitrarios en directorios del sistema con privilegios elevados.

Aunque Cisco abordó CVE-2020-3153 en febrero de 2020, se envió una solución para CVE-2020-3433 en agosto de 2020.

> *«En octubre de 2022, el equipo de respuesta a incidentes de seguridad de productos de Cisco se dio cuenta de un intento adicional de explotación de la vulnerabilidad en la naturaleza»*, dijo la compañía.

> *«Cisco continúa recomendando encarecidamente que los clientes actualicen a una versión de software fija para remediar la vulnerabilidad».*

La alerta se produce cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) se movió para agregar las dos vulnerabilidades a su catálogo de vulnerabilidades explotadas conocidas (KEV), junto con cuatro errores en los controladores GIGABYTE, citando evidencia de abuso activo en la naturaleza.

Las vulnerabilidades, a las que se les asignaron los identificadores CVE-2018-19329, CVE-2018-19321, CVE-2018-19322 y CVE-2018-19323, y parcheadas en mayo de 2020, podrían permitir que un atacante aumente los privilegios y ejecute código malicioso para tomar el control completo de un sistema afectado.

El desarrollo también sigue a un informe completo publicado por Group-IB con sede en

Singapur la semana pasada, que detalla las tácticas adoptadas por un grupo de ransomware de habla rusa denominado OldGremlin en sus ataques dirigidos a entidades que operan en el país.

El principal de sus métodos para obtener acceso inicial es la explotación de las fallas de Cisco AnyConnect mencionadas anteriormente, con las debilidades del controlador GIGABYTE empleadas para desarmar el software de seguridad, el último de los cuales también fue utilizado por el grupo de ransomware BlackByte.