La Agencia de Seguridad Cibernética e Infraestructura de los Estados Unidos (CISA) incluyó el jueves en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) una falla de seguridad ya corregida que afecta al software Cisco Adaptive Security Appliance (ASA) y Firepower Threat Defense (FTD), tras recibir informes de posibles exploits en ataques de ransomware Akira.

La vulnerabilidad en cuestión es la CVE-2020-3259 (puntuación CVSS: 7.5), una cuestión de divulgación de información de alta gravedad que permitiría a un atacante recuperar el contenido de la memoria en un dispositivo afectado. Cisco solucionó este problema como parte de las actualizaciones lanzadas en mayo de 2020.

A finales del mes pasado, la firma de ciberseguridad Truesec afirmó haber encontrado pruebas que sugieren que esta vulnerabilidad ha sido utilizada por actores del ransomware Akira para comprometer múltiples dispositivos vulnerables de Cisco Anyconnect SSL VPN durante el último año.

> *«En el caso de CVE-2020-3259, no existe un código de explotación disponible públicamente, lo que significa que un actor de amenazas, como Akira, que esté explotando esa vulnerabilidad, debería adquirir o producir su propio código de explotación, lo cual requiere un profundo conocimiento de la vulnerabilidad»,* mencionó el investigador de seguridad Heresh Zaremand.

Según Palo Alto Networks Unit 42, Akira se encuentra entre los 25 grupos que establecieron sitios de filtración de datos en 2023, y el grupo de ransomware ha afirmado públicamente haber afectado a casi 200 víctimas. Descubierto por primera vez en marzo de 2023, se cree que este grupo tiene vínculos con el conocido sindicato Conti, ya que ha enviado los ingresos de los rescates a direcciones de billeteras afiliadas a Conti.

En el último trimestre de 2023, solo este grupo delictivo enumeró 49 víctimas en su portal de filtración de datos, situándose detrás de LockBit (275), Play (110), ALPHV/BlackCat (102), NoEscape (76), 8Base (75) y Black Basta (72).

Las agencias del Poder Ejecutivo Civil Federal (FCEB) deben corregir las vulnerabilidades identificadas antes del 7 de marzo de 2024, para proteger sus redes contra posibles amenazas.

CVE-2020-3259 no es la única vulnerabilidad explotada para distribuir ransomware. A principios de este mes, Arctic Wolf Labs reveló el abuso de CVE-2023-22527, una debilidad recién descubierta en Atlassian Confluence Data Center y Confluence Server, para desplegar el ransomware C3RB3R, así como mineros de criptomonedas y troyanos de acceso remoto.

Este desarrollo ocurre al mismo tiempo que el Departamento de Estado de EE. UU. anunció recompensas de hasta $10 millones por información que pueda llevar a la identificación o localización de miembros clave del grupo de ransomware BlackCat, y hasta $5 millones por información que conduzca al arresto o condena de sus afiliados.

El esquema de ransomware como servicio (RaaS), al igual que Hive, comprometió a más de 1,000 víctimas a nivel mundial, generando al menos $300 millones en ganancias ilícitas desde su aparición a finales de 2021. Fue interrumpido en diciembre de 2023 como resultado de una operación coordinada a nivel internacional.

El panorama del ransomware se ha convertido en un mercado lucrativo, atrayendo la atención de ciberdelincuentes en busca de ganancias financieras rápidas, lo que ha llevado al surgimiento de nuevos actores como Alpha (sin confundir con ALPHV) y Wing.

A finales de enero de 2024, la Oficina de Responsabilidad del Gobierno de EE. UU. (GAO) emitió un informe que insta a una supervisión mejorada de las prácticas recomendadas para abordar el ransomware, específicamente dirigido a organizaciones de sectores críticos como manufactura, energía, atención médica y salud pública, y sistemas de transporte.