Una vulnerabilidad en Cisco Adaptive Security Appliance (ASA), que fue abordada por la compañía el pasado mes de octubre y nuevamente a inicios de abril, ha estado bajo ataques activos la naturaleza luego del lanzamiento del código de explotación de prueba de concepto (PoC).

El PoC fue publicado por los investigadores de la compañía de seguridad Positive Technologies el 24 de junio, después de lo cual, surgieron informes de que los atacantes están buscando el exploit para la vulnerabilidad.

> *«Tenable también ha recibido un informe de que los atacantes están explotando CVE-2020-3580 en la naturaleza»,* dijo la compañía.

Rastreada como CVE-2020-3580 con una puntuación CVSS de 6.1, la vulnerabilidad se refiere a múltiples fallas en la interfaz de servicios web del software Cisco ASA y el software Cisco Firepower Threat Defense (FTD), que podrían permitir que un atacante remoto no autenticado ataques de secuencias de comandos entre sitios (XSS) en un dispositivo afectado.

En junio de 2020, existían poco más de 85 mil dispositivos ASA/FTD, de los cuales, 398 se distribuyen en el 17% de las empresas Fortune 500, según la compañía de seguridad Rapid7.

La explotación exitosa, como los escenarios en los que un usuario de la interfaz está convencido de hacer clic en un enlace especialmente diseñado, podría permitir al adversario ejecutar código JavaScript arbitrario en el contexto de la interfaz o acceder a información confidencial basada en el navegador.

Aunque Cisco corrigió la vulnerabilidad en octubre de 2020, la compañía de determinó posteriormente que la solución estaba *«incompleta»,* por lo que requirió una segunda ronda de parches que se lanzaron el 28 de abril de 2021.

Debido a la disponibilidad pública del PoC, es recomendable que las empresas den prioridad

alta a la aplicación de parches para CVE-2020-3580 para mitigar el riesgo asociado a la vulnerabilidad.