El lunes, Cisco actualizó un aviso de seguridad para alertar a sus usuarios sobre la explotación activa de una vulnerabilidad presente en su Adaptive Security Appliance (ASA) desde hace más de una década.

La falla, identificada como CVE-2014-2120 (con una puntuación CVSS de 4.3), se origina en una validación insuficiente de datos en la página de inicio de sesión de WebVPN del ASA. Esto podría permitir que un atacante remoto, sin necesidad de autenticación, lleve a cabo un ataque de cross-site scripting (XSS) contra un usuario específico del dispositivo.

> *«Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario para que acceda a un enlace malicioso»,* explicó Cisco en un boletín publicado originalmente en marzo de 2014.

A partir del 2 de diciembre de 2024, la compañía ha actualizado su informe señalando que se han detectado nuevos intentos de explotación de esta vulnerabilidad en entornos reales.

Este anuncio surge poco después de que la firma de ciberseguridad CloudSEK informara que los actores detrás del malware AndroxGh0st están utilizando una amplia gama de vulnerabilidades en aplicaciones accesibles desde internet, incluida CVE-2014-2120, para facilitar la propagación del malware.

Además, esta actividad maliciosa incluye el uso de la botnet Mozi, que permite ampliar su tamaño y alcance operativos.

En respuesta, la Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) agregó esta vulnerabilidad a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) el mes pasado, exigiendo a las agencias del Ramo Ejecutivo Civil Federal (FCEB) que tomen medidas correctivas antes del 3 de diciembre de 2024.

Se recomienda encarecidamente a los usuarios de Cisco ASA mantener sus sistemas actualizados para garantizar una protección eficaz frente a posibles amenazas cibernéticas.