Cisco ha implementado actualizaciones de seguridad para abordar una vulnerabilidad crítica reportada en el motor antivirus de código abierto ClamAV, que podría conducir a la ejecución remota de código en dispositivos susceptibles.

Rastreada como CVE-2023-20032 (puntuación CVSS: 9.8), la vulnerabilidad se relaciona con un caso de ejecución remota de código que reside en el componente analizador de archivos HSF+.

La vulnerabilidad afecta a las versiones 1.0.0 y anteriores, 0.105.1 y anteriores, y 0.103.7 y anteriores. Al ingeniero de seguridad de Google, Simon Scannell, se le atribuye el descubrimiento y la notificación del error.

> *«Esta vulnerabilidad se debe a la falta de una verificación del tamaño del búfer que puede resultar en una escritura de desbordamiento del búfer del montón. Un atacante podría explotar esta vulnerabilidad enviando un archivo de partición HFS+ diseñado para que ClamAV lo escanee en un dispositivo afectado»,* dijo Cisco Talos.

La explotación exitosa de la vulnerabilidad podría permitir que un atacante ejecute código arbitrario con los mismos privilegios que el proceso de escaneo de ClamAV, o bloquee el proceso, lo que resultaría en una condición de denegación de servicio (DoS).

El equipo de red dijo que los siguientes productos son vulnerables:

- Secure Endpoint, anteriormente Advanced Malware Protection (AMP) para Endpoints (Windows, macOS y Linux)
- Nube privada segura para terminales
- Dispositivo web seguro, anteriormente Dispositivo de Seguridad Web

Además, confirmó que la vulnerabilidad no afecta a los productos Secure Email Gateway (antes Email Security Appliance) y Secure Email and Web Manager (antes Security Management Appliance).

Cisco también corrigió una vulnerabilidad de fuga de información remota en el analizador de archivos DMG de ClamAV (CVE-2023-20052, puntaje CVSS: 5.3) que podría ser explotada por un atacante remoto no autenticado.

> *«Esta vulnerabilidad se debe a la habilitación de la sustitución de entidades XML que puede resultar en la inyección de entidades externas XML. Un atacante podría explotar esta vulnerabilidad al enviar un archivo DMG diseñado para que ClamAV lo escanee en un dispositivo afectado»,* dijo Cisco.

Cabe mencionar que CVE-2023-20052 no afecta a Cisco Secure Web Appliance. Ambas vulnerabilidades se solucionaron en las versiones 0.103.0, 0.105.2 y 1.0.1 de ClamAV.

Cisco también resolvió por separado una vulnerabilidad de denegación de servicio (DoS) que afectaba a Cisco Nexus Dashboard (CVE-2023-20014, puntaje CVSS: 7.5) y otras dos vulnerabilidades de escalada de privilegios e inyección de comandos en Email Security Appliance (ESA) y Secure Email y Administrador Web (CVE-2023-20009 y CVE-2023-20075, puntaje CVSS: 6.5).