Sophos y SonicWall han emitido alertas sobre fallos de seguridad críticos en Sophos Firewall y en los dispositivos Secure Mobile Access (SMA) de la serie 100, los cuales podrían ser aprovechados para ejecutar código de forma remota.

Los dos fallos que afectan a Sophos Firewall se describen a continuación:

- *CVE-2025-6704 (puntuación CVSS: 9.8)* – Una vulnerabilidad que permite escritura arbitraria de archivos en la función Secure PDF eXchange (SPX) podría permitir ejecución remota de código antes de la autenticación, si se utiliza una configuración específica de SPX junto con el firewall operando en modo de Alta Disponibilidad (HA).
- *CVE-2025-7624 (puntuación CVSS: 9.8)* – Una falla de inyección SQL en el antiguo proxy SMTP en modo transparente puede facilitar la ejecución remota de código si hay una política de cuarentena activa para correos electrónicos y el sistema fue actualizado desde una versión anterior a la 21.0 GA.

Sophos indicó que *CVE-2025-6704* afecta aproximadamente al 0.05% de los dispositivos, mientras que *CVE-2025-7624* impacta hasta el 0.73%. Ambas vulnerabilidades han sido corregidas junto con otra falla de alta gravedad, una inyección de comandos en el componente WebAdmin (*CVE-2025-7382*, *puntuación CVSS: 8.8*), que podría permitir la ejecución de código previa a la autenticación en dispositivos auxiliares bajo configuración HA, si la autenticación OTP está activada para el usuario administrador.

La empresa también solucionó otras dos vulnerabilidades:

- *CVE-2024-13974 (puntuación CVSS: 8.1)* – Una debilidad de lógica empresarial en el componente Up2Date que permitiría a un atacante manipular el entorno DNS del firewall y ejecutar código remotamente.
- *CVE-2024-13973 (puntuación CVSS: 6.8)* – Una vulnerabilidad de inyección SQL post-autenticación en WebAdmin que podría ser explotada por administradores para ejecutar código arbitrario.

El *Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC)* fue acreditado como

descubridor y reportante tanto de *CVE-2024-13974* como de *CVE-2024-13973*. Las versiones afectadas son las siguientes:

- *CVE-2024-13974* – Afecta a Sophos Firewall v21.0 GA (21.0.0) y anteriores
- *CVE-2024-13973* – Afecta a Sophos Firewall v21.0 GA (21.0.0) y anteriores
- *CVE-2025-6704* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores
- *CVE-2025-7624* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores
- *CVE-2025-7382* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores

La divulgación coincide con el informe de SonicWall sobre una vulnerabilidad crítica en la interfaz web de administración de la serie SMA 100 (*CVE-2025-40599, puntuación CVSS: 9.1*), que puede permitir a un atacante remoto con privilegios administrativos subir archivos arbitrarios y lograr ejecución remota de código.

Este fallo afecta a los productos SMA 100 Series (SMA 210, 410, 500v) y ya ha sido corregido en la versión 10.2.2.1-90sv.

SonicWall también señaló que, aunque no se ha detectado explotación activa, existe un riesgo potencial debido a un informe reciente del *Google Threat Intelligence Group (GTIG)*, el cual reveló que un actor de amenazas conocido como *UNC6148* ha utilizado dispositivos SMA 100 completamente actualizados para desplegar una puerta trasera llamada *OVERSTEP*.

Además de aplicar los parches disponibles, la compañía recomienda a los usuarios de dispositivos SMA 100 Series implementar las siguientes medidas:

- Deshabilitar el acceso de administración remota en la interfaz externa (X1) para reducir la superficie de ataque
- Restablecer todas las contraseñas y volver a vincular el OTP (One-Time Password) para usuarios y administradores del dispositivo
- Aplicar autenticación multifactor (MFA) para todos los usuarios
- Activar el Firewall de Aplicaciones Web (WAF) en los dispositivos SMA 100

También se aconseja a las organizaciones que revisen los registros del dispositivo y el historial de conexiones en busca de actividades sospechosas o accesos no autorizados.

En el caso del producto virtual *SMA 500v*, se requiere realizar una copia de seguridad del archivo OVA, exportar la configuración, eliminar la máquina virtual y todos sus discos y snapshots asociados, instalar nuevamente el OVA desde SonicWall usando un hipervisor y restaurar la configuración.