
Akira Ransomware explora falha de um ano da SonicWall com vários vetores

Data: 2025-09-11 20:54:46

Autor: Inteligência Against Invaders

Akira Ransomware explora falha de um ano da SonicWall com vários vetores

Os pesquisadores alertam que o grupo de ransomware Akira está explorando uma falha de firewall da SonicWall de um ano, provavelmente usando três vetores de ataque para acesso inicial.

O [Grupo de ransomware Akira](#) está explorando uma vulnerabilidade de firewall SonicWall de um ano, rastreada como [CVE-2024-40766](#) (pontuação CVSS de 9,3), provavelmente usando três vetores de ataque para acesso inicial, de acordo com o Rapid7.

“As evidências coletadas durante as investigações da Rapid7 sugerem que o grupo Akira está potencialmente utilizando uma combinação de todos esses três riscos de segurança para obter acesso não autorizado e conduzir operações de ransomware.” lê o [relatório](#) publicado pela Rapid7.

A vulnerabilidade é um problema de controle de acesso impróprio que reside no acesso de gerenciamento do SonicWall SonicOS. Um invasor pode explorar o problema para obter acesso não autorizado aos dispositivos.

A SonicWall abordou a falha crítica em seus firewalls em agosto de 2024, e a CISA dos EUA [Adicionado](#) ele para o seu [Catálogo de vulnerabilidades exploradas conhecidas \(KEV\)](#) em setembro de 2024.

Em agosto de 2025, a SonicWall [investigado alegações de um dia zero](#) sendo usado em ataques de ransomware, mas não encontrou evidências de qualquer nova vulnerabilidade em seus produtos.

A SonicWall lançou a investigação após um aumento na [Ataques ransomware Akira](#) visando firewalls Gen 7 com SSLVPN habilitado. A empresa trabalhou para determinar se os incidentes decorrem de uma falha existente ou de uma vulnerabilidade recém-descoberta.

A SonicWall confirmou mais tarde que não há dia zero envolvido em ataques recentes de ransomware, mas sim a exploração de uma falha conhecida, [CVE-2024-40766](#). Embora muitos sistemas tenham sido corrigidos, os invasores ainda podem acessá-los se as credenciais não forem alteradas. Menos de 40 incidentes relacionados estão sob investigação da SonicWall, principalmente ligados a migrações de firewall.

*“Agora temos grande confiança de que a recente atividade do SSLVPN é **não conectado a uma vulnerabilidade de dia zero**. Em vez disso, há uma correlação significativa com a atividade de ameaças relacionada ao CVE-2024-40766, que foi divulgada anteriormente e documentada em*

nosso comunicado público [SNWLID-2024-0015](#).” lê o [Consultivo](#) publicado pelo fornecedor de segurança.

“Atualmente, estamos investigando menos de 40 incidentes relacionados a essa atividade cibernética. Muitos dos incidentes estão relacionados a migrações de firewalls Gen 6 para Gen 7, em que as senhas de usuários locais foram transferidas durante a migração e não redefinidas. A redefinição de senhas foi uma etapa crítica descrita no [Assessoria Original](#). “

A SonicWall emitiu novas orientações sobre o risco do grupo de usuários padrão SSLVPN, que pode conceder acesso não autorizado em determinadas configurações LDAP. O Rapid7 também encontrou agentes de ameaças abusando do Portal do Virtual Office para configurar MFA/TOTP com credenciais expostas. As evidências sugerem que o ransomware Akira está explorando uma mistura dessas falhas para ataques.

“As evidências coletadas durante as investigações da Rapid7 sugerem que o grupo Akira está potencialmente utilizando uma combinação de todos esses três riscos de segurança para obter acesso não autorizado e conduzir operações de ransomware.” continua o relatório.

A Rapid7 recomenda que os usuários da SonicWall protejam contas, habilitem a MFA, corrijam o risco de grupos padrão SSLVPN, restrinjam e monitorem o Portal do Virtual Office e apliquem patches de segurança.

O [Akira ransomware](#) está ativo desde março de 2023, os agentes de ameaças por trás do malware afirmam já ter hackeado várias organizações em vários setores, incluindo educação, finanças e imóveis. Como outras gangues de ransomware, o grupo desenvolveu um criptografador Linux para atingir servidores VMware ESXi.

Siga-me no Twitter: [@securityaffairs](#) e [Linkedine](#) [Mastodonte](#)

[PierluigiPaganini](#)

([Assuntos de Segurança](#)—hacking,Akira ransomware)
