A SonicWall avisa os clientes para redefinir as credenciais depois que os

Data: 2025-09-18 14:55:19

Autor: Inteligência Against Invaders

A SonicWall avisa os clientes para redefinir as credenciais depois que os backups da MySonicWall foram expostos

A SonicWall pede aos usuários que redefinam as credenciais depois que os backups do MySonicWall forem expostos; A empresa bloqueou os agentes da ameaça e notificou as autoridades.

A SonicWall pediu aos clientes que redefinissem as credenciais depois que os arquivos de backup do firewall vinculados às contas da MySonicWall foram expostos. A empresa anunciou que bloqueou o acesso dos invasores e está trabalhando com especialistas em segurança cibernética e agências de aplicação da lei para determinar o escopo da violação.

A SonicWall diz que menos de 5% dos clientes foram afetados, nenhum arquivo vazou, mas a violação ainda apresenta riscos que precisam de ação urgente.

“As equipes de segurança da SonicWall detectaram recentemente atividades suspeitas direcionadas ao serviço de backup em nuvem para firewalls, o que confirmamos como um incidente de segurança nos últimos dias. Nossa investigação descobriu que os agentes de ameaças acessaram arquivos de preferência de firewall de backup armazenados na nuvem por menos de 5% de nossa base instalada de firewall. Embora as credenciais nos arquivos tenham sido criptografadas, os arquivos também incluíam informações que poderiam tornar mais fácil para os invasores explorar potencialmente o firewall relacionado.” lê o declaração *publicado pela empresa.*

“No momento, não temos conhecimento de que esses arquivos vazaram online por agentes de ameaças. Este não foi um ransomware ou evento semelhante para a SonicWall, mas sim uma série de ataques de força bruta destinados a obter acesso aos arquivos de preferência armazenados no backup para uso potencial por agentes de ameaças.”

O incidente afetou os firewalls da SonicWall com backup de arquivos de preferência em MySonicWall.com

A SonicWall recomenda que os clientes façam login em suas contas MySonicWall e verifiquem se os backups na nuvem estão ativados. Se não, não há risco. Em caso afirmativo, procure por números de série sinalizados, eles indicam firewalls afetados que precisam de correção imediata. Se você usou backups, mas não vê nenhum dispositivo sinalizado, a SonicWall compartilhará mais orientações em breve.

A empresa disse aos clientes afetados para importar novos arquivos de preferência. No entanto, a importação do novo arquivo interrompe VPNs IPSec, associações TOTP e acesso do usuário. Após

a importação, os usuários devem reconfigurar as chaves pré-compartilhadas da VPN e redefinir o TOTP junto com as senhas do usuário. Para reduzir o tempo de inatividade, a SonicWall recomenda importar durante janelas de manutenção, fora do horário comercial ou períodos de baixa atividade, pois o processo reinicializa o firewall imediatamente.

“O arquivo de preferências modificado fornecido pela SonicWall foi criado a partir do arquivo de preferências mais recente encontrado no armazenamento em nuvem”, a empresa diz*. “Essas alterações de configuração foram feitas para atualizar esses parâmetros possivelmente expostos e fornecer uma configuração que você pode achar útil para correção”*

SonicWall diz que os clientes não podem importar novos arquivos de preferência devem seguir seu **orientação** para redefinir manualmente as credenciais no SonicOS.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,violação de segurança)