Citrix Falha de 0 dias sob exploração ativa desde maio

Data: 2025-08-30 09:47:14

Autor: Inteligência Against Invaders

O pesquisador de segurança Kevin Beaumont revelou detalhes alarmantes sobre a CVE-2025-6543,

uma vulnerabilidade crítica do Citrix NetsCaler que foi ativamente explorada como um ataque de dia

zero por meses antes da emissão da empresa.

O que a Citrix subestimou inicialmente como uma simples vulnerabilidade de “negação de serviço” provou ser uma falha sofisticada de execução de código remoto que comprometeu o governo e os serviços jurídicos em todo o mundo.

A vulnerabilidade, que permite que os invasores atinjam a execução remota de código por meio de ataques de transbordamento de memória, está sob exploração ativa desde pelo menos no início de maio de 2025, de acordo com investigações da NCSC Holanda.

Somente Citrix lançado Patches em 25 de junho de 2025, o que significa que os atores de ameaças tinham meses para explorar sistemas não patches antes que a vulnerabilidade se tornasse conhecimento público.

As principais características do ataque incluem:

- Certificados de clientes maliciosos enviados ao NetsCaler Endpoint /cgi/api/login através de centenas de solicitações de postagem.
- Ataques de transbordamento de memória projetados para substituir os pedaços de memória e executar o código arbitrário.
- Implantação de webshells e backdoors persistentes que permanecem ativos mesmo após o patch.
- O apagamento ativo dos traços de ataque para complicar investigações forenses.
- Exploração de várias vulnerabilidades Citrix simultaneamente, incluindo CVE-2025-5777 (Citrixbleed 2).

A metodologia de ataque envolve o envio de certificados de clientes maliciosos para o terminal NetScaler /cgi/api/login Através de centenas de solicitações de postagem projetadas para substituir os pedaços de memória e executar o código arbitrário.

O que torna isso particularmente preocupante é que os invasores estão implantando webshells e backdoors persistentes que permanecem ativos mesmo após o patch, garantindo o acesso contínuo a redes comprometidas.

A NCSC Holanda relatou que “várias organizações críticas da Holanda foram atacadas com sucesso”, com investigações forenses revelando que os atacantes apagaram ativamente traços de sua atividade para complicar os esforços de resposta a incidentes.

Os mesmos atores de ameaças parecem estar explorando várias vulnerabilidades Citrix simultaneamente, incluindo CVE-2025-5777 (Citrixbleed 2) para roubar sessões de usuário e ignorar a autenticação de vários fatores.

Impacto generalizado, resposta fraca

O escopo desta campanha se estende muito além das estimativas iniciais, com agências governamentais, serviços jurídicos e organizações críticas de infraestrutura em todo o mundo vítimas a esses ataques.

Os sistemas comprometidos foram usados ??como pontos de lançamento para o movimento lateral em ambientes do Active Directory, com os invasores usando indefinições de credenciais da conta de serviço LDAP para expandir o acesso à rede.

A avaliação de impacto revela:

- Agências governamentais, serviços jurídicos e organizações críticas de infraestrutura comprometidas em todo o mundo.
- Movimento lateral em ambientes do Active Directory usando credenciais de conta de serviço LDAP roubadas.
- Voltado para a Internet Dispositivos NetsCaler diminuiu pela metade desde o final de 2023 devido a preocupações de segurança.
- Os clientes confiam cada vez mais nas agências governamentais, em vez de na Citrix para obter inteligência de ameaças.
- Condições restritivas colocadas nos clientes solicitando scripts de detecção da Citrix.

A resposta de Citrix à crise atraiu críticas fortes de especialistas em segurança. A empresa forneceu aos clientes scripts de detecção apenas mediante solicitação e em condições restritivas, enquanto não comunica a verdadeira severidade e escopo da vulnerabilidade.

Essa falta de transparência deixou os clientes incapazes de avaliar adequadamente seu status de compromisso ou implementar medidas defensivas adequadas.

A telemetria de segurança da Shodan indica que os dispositivos NetScaler voltados para a Internet diminuíram pela metade desde o final de 2023, sugerindo que as organizações estão abandonando a plataforma devido a preocupações de segurança em andamento.

A situação se tornou tão problemática que os clientes confiam cada vez mais nas agências de segurança cibernética do governo e pesquisadores independentes, em vez de serem a própria Citrix para obter uma inteligência precisa das ameaças.

As organizações que executam os sistemas Citrix NetsCaler precisam tomar medidas imediatas para proteger sua infraestrutura.

Especialistas em segurança recomendam verificar os logs de acesso à web para obter solicitações de postagem suspeitas para /cgi/api/login terminais, particularmente aqueles acompanhados pelo código de erro 1245184, o que indica certificados de clientes inválidos.

As medidas de resposta crítica incluem:

- Verifique os logs de acesso à web para obter solicitações de postagem suspeitas para /cgi/api/login pontos de extremidade.
- Procure o código de erro 1245184 indicando certificados de clientes inválidos em logs NetsCaler.
- Os dispositivos NetScaler afetados pela energia afetados imediatamente se forem suspeitos de compromisso.
- Realize imagens forenses usando scripts de detecção da NCSC Holanda disponíveis no GitHub.
- Altere todas as credenciais da conta de serviço LDAP associadas.
- Implantar sistemas de reposição com novas credenciais, em vez de tentar reparos.

O NCSC Holanda publicou scripts abrangentes de detecção e ferramentas forenses no Github para ajudar as organizações a identificar indicadores de compromisso e conduzir a resposta adequada dos incidentes.

As organizações que descobrem sinais de exploração devem desligar imediatamente os dispositivos afetados do NetScaler, conduzir imagens forenses, alterar todas as credenciais de conta de serviço LDAP associadas e implantar sistemas de reposição com novas credenciais.

A crise destaca problemas sistêmicos mais amplos com a segurança do NetScaler, pois a plataforma sofreu múltiplos Explorações de dias zero Nos últimos meses.

Com os atores de ameaças “em execução em torno do produto regularmente” e Citrix não fornecendo transparência adequada, as organizações podem precisar considerar soluções alternativas de acesso remoto para proteger sua infraestrutura crítica de ataques contínuos.

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**