BOLETIM DE SEGURANÇA

MITRE Corporation foi alvo de ataque de zero day em dispositivos Ivanti Connect Secure

heimdall
security research
A DIVISION OF ISH

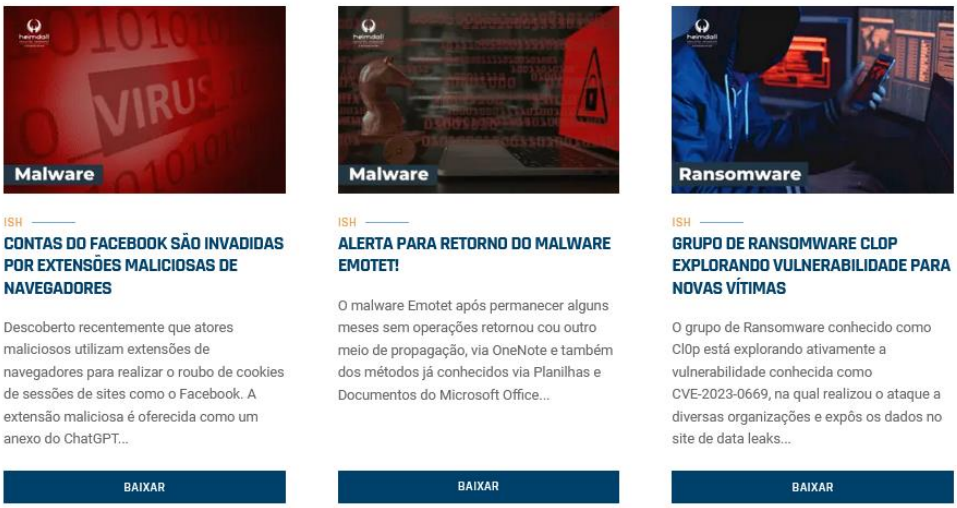
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A MITRE Corporation informou que foi comprometida por um ataque patrocinado pelo estado, que se aproveitou de duas vulnerabilidades CVE-2023-46805 e CVE-2024-21887, nos dispositivos Ivanti Connect Secure desde janeiro de 2024. Esse ataque resultou na violação do NERVE, o ambiente de experimentação, pesquisa e virtualização em rede da empresa, que é utilizado para fins de pesquisa e desenvolvimento de protótipos.

2 INFORMAÇÕES SOBRE A AMEAÇA

O pesquisador de segurança cibernética Lex Crumpton, informou que desde janeiro de 2024, um ator malicioso realizou o reconhecimento nas redes, explorando duas falhas críticas inéditas no Ivanti Connect Secure para acessar uma VPN. Eles conseguiram evitar a autenticação multifatorial por meio de sequestro de sessão. Posteriormente, realizaram movimentos laterais e penetraram mais fundo na infraestrutura VMware da rede, utilizando uma conta de administrador que havia sido comprometida. Para manter acesso e extrair credenciais, utilizaram uma mistura de backdoors e webshells avançados.

Embora a MITRE tenha adotado as melhores práticas, seguido orientações de fornecedores e conselhos governamentais para atualizar e reforçar o sistema Ivanti, o movimento lateral na infraestrutura VMware passou despercebido. Naquele momento, acreditava-se que todas as medidas necessárias para mitigar a vulnerabilidade haviam sido implementadas, mas ficou evidente que não foram suficientes.

Technique Title	ID	Use
Initial Access		
Exploit Public-Facing Applications	T1190	Adversary compromised MITRE's prototype network through a pair of zero-day vulnerabilities in Ivanti Connect Secure (CVE-2023-46805, CVE-2024-21887)
Persistence		
Server Software Component: Web Shell	T1505.003	Adversary installed webshells to maintain persistence
Execution		
Command and Scripting Interpreter	T1059	Adversary executed commands and scripts
Lateral Movement		
Remote Service Session Hijacking	T1563	Adversary hijacked Pulse sessions for users to move laterally into the VMware environment, bypassing Multi-Factor Authentication
Remote Services	T1021	Adversary attempted several different methods (i.e. RDP and SSH) to utilize valid accounts and move across the network
Valid Accounts	T1078	Adversary leveraged compromised accounts
Exfiltration		
Exfiltration Over C2 Channel	T1041	Adversary exfiltrated data using their C2 infrastructure
Defense Evasion		
Hide Artifacts: Run Virtual Instance	T1564.006	Adversary created staging and persistent VMs within VMware environment.

Figura 1 – Técnicas ATT&CK observadas.

O ataque foi caracterizado pelo uso indevido de duas vulnerabilidades significativas, CVE-2023-46805 e CVE-2024-21887, respectivamente. Estas brechas de segurança permitiram aos atacantes não só contornar sistemas de autenticação, mas também executar comandos arbitrários nos sistemas afetados.

Após garantir um ponto de entrada, os atores exploraram a infraestrutura VMware, utilizando credenciais de um administrador previamente comprometidas, o que facilitou a instalação de backdoors e web shells para manter acesso e extrair credenciais valiosas.

A MITRE, assegurou que a NERVE, uma rede colaborativa que provê recursos de armazenamento, computação e rede, não teve sua integridade comprometida, assim como a rede corporativa principal e os sistemas associados a parceiros. Ações imediatas foram implementadas pela organização para mitigar o incidente, incluindo procedimentos de resposta e recuperação, além de análises forenses detalhadas para avaliar o impacto do ataque. A Volexity identificou o grupo UTA0178, supostamente vinculado ao governo chinês, como responsável pela exploração inicial das vulnerabilidades. A Mandiant observou que outros coletivos hackers chineses seguiram o exemplo e começaram a explorar as mesmas falhas de segurança.

Após a detecção da violação, foi implementado um plano de resposta coordenada em que necessita-se efetuar o isolamento dos sistemas e segmentos de rede comprometidos para impedir a propagação do ataque. Ajustes nas regras de firewall não eram suficientes devido à conectividade da rede com laboratórios corporativos, exigindo o desligamento da infraestrutura de acesso e isolamento de sistemas periféricos. Um inventário de rede detalhado foi crucial para a contenção rápida. A recuperação efetiva demanda um conselho de administração e equipe de gestão coesos. O conselho do MITRE estabeleceu um comitê ad hoc para governança e supervisão. O CTO liderou a resposta corporativa, harmonizando as ações do CIO e CISO, a liderança de unidade de negócios, a recuperação de projetos e as equipes de comunicação e consultoria jurídica.

Deu-se início a múltiplas análises forenses para determinar o alcance do comprometimento, as técnicas dos adversários e a extensão do ataque. A coleta de logs confiáveis foi essencial para a investigação, que ainda está em andamento. Com os sistemas comprometidos contidos, necessita-se de novos recursos de TI para os projetos. Identificamos rapidamente alternativas, realizamos auditorias de segurança e estabelecer procedimentos de migração. Projetos prioritários foram restabelecidos em ambientes seguros.

3 RECOMENDAÇÕES

Conforme a investigação, alguns recursos adicionais foram disponibilizados para reforçar a infraestrutura contra os TTPs identificados no incidente. No entanto, recomenda-se estratégias preventivas para fortalecer as redes:

Autenticação forte

- Adote controles de acesso avançados, incluindo autenticação multifatorial robusta e princípios de menor privilégio.

Gerenciamento regular de patches

- Atualize sistemas e softwares regularmente para corrigir vulnerabilidades conhecidas.

Acesso com privilégio mínimo

- Limite os privilégios dos usuários para reduzir o risco associado a credenciais comprometidas.

Segmentação de rede

- Utilize a segmentação para diminuir o alcance de violações e restringir atividades mal-intencionadas.

Avaliações de vulnerabilidade

- Conduza avaliações e testes de penetração frequentes para proativamente identificar e corrigir falhas de segurança.

Programa de inteligência de ameaças

- Mantenha-se informado e aja conforme as orientações de fontes confiáveis, como os alertas da CISA, que fornecem técnicas de detecção e mitigação.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Mitre
- Medium
- Thehackernews

heimdall
security research
A DIVISION OF ISH