BOLETIM DE SEGURANÇA

Ator de ameaça vendendo exploração do VMware ESXi Shell em fórum hacker

heimdall
security research
A DIVISION OF ISH

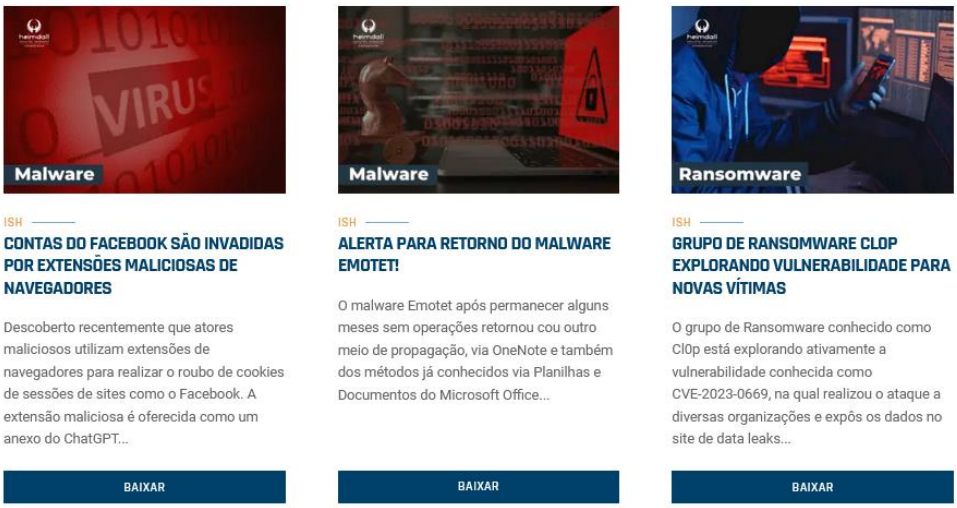
TLP: CLEAR

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

Recentemente foi observado em fórum hacker, um ator de ameaça realizando a venda de uma possível exploração direcionada ao ***VMware ESXi Shell Service***. O ESXi Shell, é um componente essencial para gerenciar hosts VMware ESXi, fornecendo uma interface de linha de comando para interação direta com o host.

2 DETALHES DA PUBLICAÇÃO

O ator de ameaça está oferecendo para venda um exploit chamado 'ESXiVortex' que tem como alvo o Serviço Shell VMware ESXi, permitindo uploads de shell remotos não autenticados. O exploit exige que o serviço de shell ESXi seja habilitado, que o IPv4 seja definido como primário e que os hosts alvos estejam rodando o vSphere ESXi 7.x/8.x. Os detalhes técnicos incluem um bypass de autenticação que leva a uploads de arquivos remotos no diretório /scratch, com um script de auto-exploração em Python incluído que realiza a geração e entrega de pacotes maliciosos. O post afirma que o exploit é uma vulnerabilidade zero-day, e o preço solicitado é de $1,500,000, conforme mostra imagem abaixo da publicação.

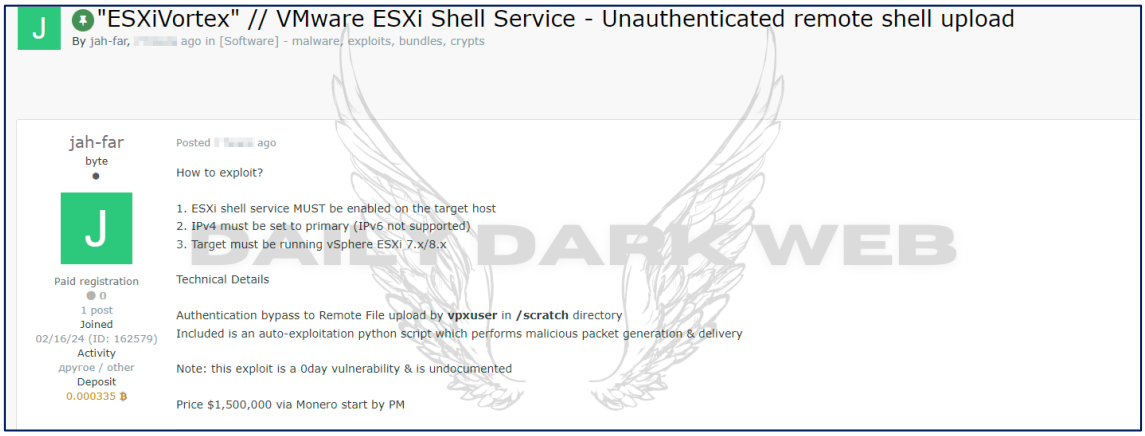


Figura 1 – Publicação de venda do ator malicioso.

O usuário *vpxuser* é uma conta de sistema empregada pelo VMware ESXi para realizar várias operações internas. O diretório /scratch serve como um espaço temporário no sistema operacional ESXi para guardar dados provisórios e de apoio. A possibilidade de um invasor descarregar arquivos desse diretório sem necessidade de autenticação representa um grave risco de segurança, uma vez que isso pode possibilitar o acesso a informações sigilosas ou a comprometimento do sistema.

3 CONCLUSÃO

O alcance das consequências desta exploração é extenso. O VMware ESXi é largamente empregado em contextos empresariais para administrar infraestruturas de servidores virtuais. Se a exploração afetar o ESXi Shell, poderia possibilitar aos invasores assumirem o controle de todas as máquinas virtuais no servidor, resultando em um amplo vazamento de dados internos e de clientes. Além disso, tal perturbação pode se estender a sistemas operacionais essenciais, provocando períodos prolongados de inatividade e impactos financeiros consideráveis para as organizações.

4 RECOMENDAÇÕES

Abaixo são elencadas pela ISH medidas de segurança visando a mitigação da referida ameaça.

Controle de acesso rigoroso

- Restrinja o acesso ao ESXi Shell e ao SSH apenas a usuários que precisem realmente utilizar esses serviços. Use listas de controle de acesso (ACLs) para definir quem pode acessar o Shell.
- Implemente autenticação multifatorial para adicionar uma camada extra de segurança ao processo de login.

Monitoramento e auditoria

- Configure e habilite logs detalhados para todas as atividades no ESXi Shell. Isso inclui comandos executados, tentativas de login e alterações de configuração.
- Utilize ferramentas de gerenciamento e monitoramento de logs, como o vRealize Log Insight da VMware, para análise contínua e alertas de atividades suspeitas.

Atualizações e patches

- Mantenha o sistema operacional ESXi e todos os componentes relacionados atualizados com as últimas versões e patches de segurança disponibilizados pela VMware. Isso ajuda a proteger contra vulnerabilidades conhecidas.

Segurança em camadas

- Utilize firewalls para bloquear acessos não autorizados ao ESXi Shell. Configure regras específicas que apenas permitam conexões de IPs confiáveis.
- Implemente soluções de detecção e prevenção de intrusos (IDS/IPS) para monitorar e bloquear atividades maliciosas.

Configurações de segurança de rede

- Use redes separadas para o tráfego de gestão e o tráfego de dados regular dos seus servidores virtuais. Isso limita a exposição do ESXi Shell a potenciais atacantes na rede.

Políticas e treinamentos de segurança

- Desenvolva e aplique políticas de segurança claras relacionadas ao uso do ESXi Shell e assegure-se de que todos os usuários e administradores estejam cientes das melhores práticas de segurança.

- Realize treinamentos regulares sobre segurança cibernética para os administradores de sistema, focando na identificação de atividades suspeitas e na resposta a incidentes.

Uso de ferramentas de segurança especializadas

- Considere o uso de ferramentas especializadas para segurança de ambientes virtualizados.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Dailydarkweb
- Gbhackers

heimdall
security research
A DIVISION OF ISH