BOLETIM DE SEGURANÇA

VMware lança patches para vulnerabilidades críticas no Cloud Foundation e vCenter Server

heimdall
security research
A DIVISION OF ISH

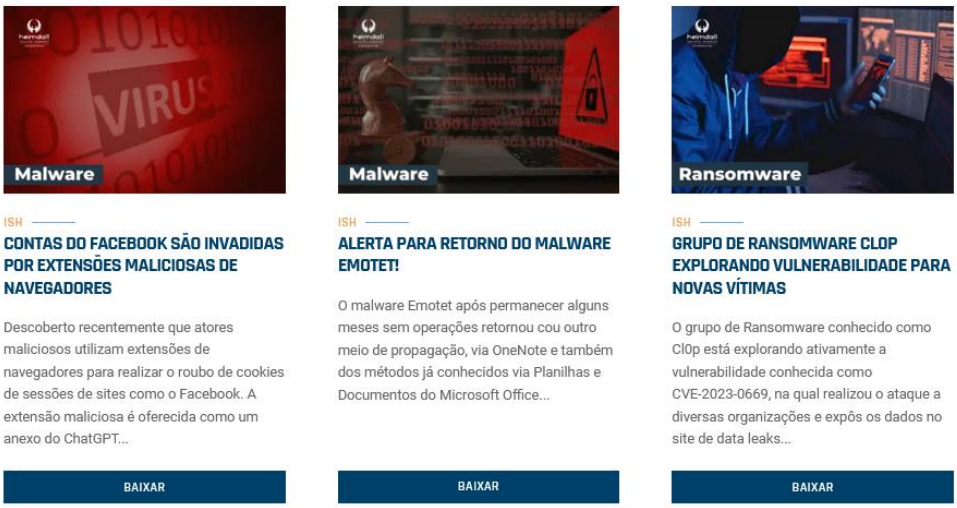
TLP: CLEAR

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

1 Sumário Executivo 4
2 Informações sobre as vulnerabilidades 5
3 Conclusão 6
4 Recomendações 7
5 Referências 8
6 Autores 9

1 SUMÁRIO EXECUTIVO

Recentemente, a VMware divulgou um alerta de segurança sobre vulnerabilidades críticas no vCenter Server. Estas falhas incluem a possibilidade de execução remota de código e escalonamento de privilégios locais. O VMware vCenter Server é uma plataforma central de gerenciamento para VMware vSphere, que facilita o controle de máquinas virtuais e hosts ESXi.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

As três vulnerabilidades informadas pela VMware foram catalogadas como:

CVE-2024-37079

- Trata-se de uma vulnerabilidade de heap overflow na implementação do protocolo DCERPC do vCenter Server. Essa falha permite que um agente malicioso com acesso à rede envie pacotes especialmente formatados, o que pode resultar na execução remota de código. (Pontuação CVSS v3.1: 9,8 “crítico”).

CVE-2024-37080

- Semelhante à CVE-2024-37079, essa vulnerabilidade também é um heap overflow no protocolo DCERPC do vCenter Server. Um invasor com acesso à rede pode explorar essa falha enviando pacotes especialmente criados, o que pode levar à execução remota de código. (Pontuação CVSS v3.1: 9,8 “crítico”).

CVE-2024-37081

- Essa vulnerabilidade decorre de uma configuração inadequada do sudo no vCenter Server. Ela permite que um usuário local autenticado explore a falha para elevar seus privilégios a nível de root no vCenter Server Appliance. (Pontuação CVSS v3.1: 7,8 “alta”).

As falhas acima afetam o **VMware vCenter Server** nas versões **7.0 e 8.0** e o **VMware Cloud Foundation** versões **4.xe 5.x**.

3 CONCLUSÃO

Nos últimos anos, os softwares da VMware têm se tornado alvos frequentes de atores maliciosos devido à sua ampla utilização em ambientes corporativos. Esses atores exploram vulnerabilidades em produtos como vSphere, vCenter e ESXi para obter acesso não autorizado a redes e sistemas. Muitas vezes, as falhas exploradas permitem a execução remota de código, escalonamento de privilégios e movimentação lateral dentro das infraestruturas virtuais, acarretando vários riscos e prejuízos financeiros para as organizações afetadas.

4 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Aplicação de patches

- Mantenha todos os sistemas VMware atualizados com os patches de segurança mais recentes. Monitore regularmente os boletins de segurança da VMware para novas vulnerabilidades e patches.

Segmentação de rede

- Implemente segmentação de rede para limitar a movimentação lateral de invasores dentro da infraestrutura. Utilize firewalls e VLANs para isolar segmentos críticos e reduzir o risco de propagação de ataques.

Autenticação e autorização fortes

- Use autenticação multifator (MFA) para todos os acessos administrativos. Garanta que apenas usuários autorizados tenham privilégios de administração e minimize o uso de contas com privilégios elevados.

Monitoramento contínuo

- Implemente soluções de monitoramento e detecção de intrusões (IDS/IPS) para identificar atividades suspeitas em tempo real. Utilize logs e ferramentas de análise para detectar comportamentos anômalos.

Configurações de segurança rígidas

- Siga as melhores práticas de configuração de segurança recomendadas pela VMware. Desative serviços e protocolos não utilizados e limite o acesso ao mínimo necessário.

Backups regulares

- Realize backups regulares e seguros das configurações e dados críticos. Teste periodicamente a restauração de backups para garantir que possam ser utilizados em caso de ataque.

Educação e treinamento

- Treine a equipe de TI e os usuários finais sobre as melhores práticas de segurança e conscientização sobre ameaças. Simulações de phishing e treinamentos periódicos podem ajudar a reduzir o risco de comprometimento por erro humano.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Broadcom**
- **NVD**
- **Bleepingcomputer**

6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH