BOLETIM DE SEGURANÇA

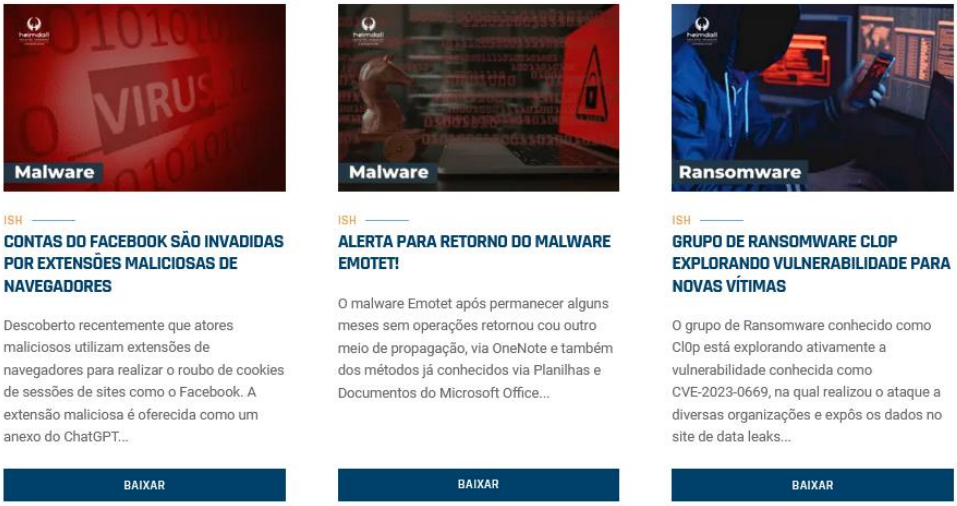
Broadcom lança correção para a vulnerabilidade CVE-2024-38812 crítica no VMware vCenter

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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

Broadcom lançou atualizações de segurança que corrige uma vulnerabilidade crítica **no VMware vCenter Server**, que poderia permitir a execução remota de código. Essa falha, representa um risco significativo para os sistemas, pois um agente malicioso pode explorá-la para comprometer a segurança de redes corporativas. A Broadcom recomenda que todas as organizações atualizem seus sistemas imediatamente para evitar possíveis ataques.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade, identificada como CVE-2024-38812, categorizada como crítica, está relacionada a um estouro de heap no protocolo DCE/RPC. De acordo com o boletim da VMware, um atacante com acesso à rede do vCenter Server pode explorar essa falha enviando um pacote de rede especialmente elaborado, resultando na execução remota de código. Essa vulnerabilidade é comparável a outras duas falhas de execução remota de código, CVE-2024-37079 e CVE-2024-37080, que a VMware abordou em junho de 2024. Além disso, outra falha de escalonamento de privilégios, agora de classificação alta CVE-2024-38813 (CVSS: 7,5), também foi corrigida. Essa falha permitiria que um atacante elevasse seus privilégios para root ao enviar pacotes maliciosos.

A VMware corrigiu esses problemas nas versões mais recentes do vCenter Server 8.0 U3b, 7.0 U3s e VMware Cloud Foundation. Embora não haja relatos de exploração ativa dessas falhas, a Broadcom recomenda a aplicação imediata dos patches para garantir a segurança.

O anúncio foi feito em meio a uma recomendação conjunta da Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA) e do FBI, pedindo que organizações corrijam vulnerabilidades de cross-site scripting (XSS). Essas falhas podem ser aproveitadas por atacantes para comprometer sistemas. Conforme o alerta, vulnerabilidades XSS surgem quando as entradas de usuários em aplicativos não são devidamente validadas, higienizadas ou escapadas pelos desenvolvedores. Segundo as agências, essa negligência permite que invasores injetem scripts maliciosos nos aplicativos, resultando em manipulação, roubo ou uso inadequado de dados em diferentes contextos.

3 RECOMENDAÇÕES

Para mitigar essa vulnerabilidade, instale as atualizações conforme as implantações impactadas.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Broadcom**
- **Thehackernews**
- **Tenable**
- **CVE_Mitre**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH