BOLETIM DE SEGURANÇA

CVE-2024-21111, PoC para falha grave no VirtualBox disponível

heimdall
security research
A DIVISION OF ISH

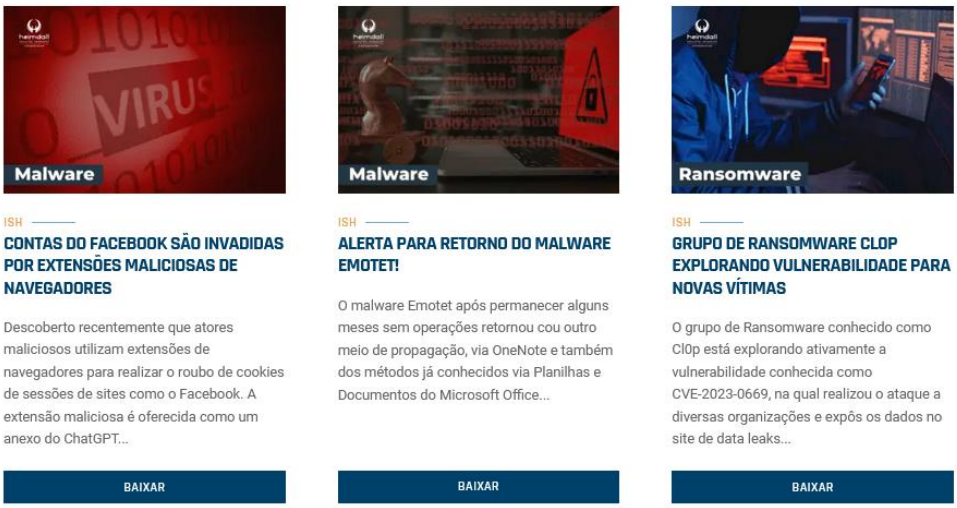
TLP: CLEAR

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

A CVE-2024-21111 é uma vulnerabilidade grave no Oracle VirtualBox, afetando versões anteriores à 7.0.16. Ela permite que atacantes com acesso básico a um sistema Windows executando o VirtualBox aumentem seus privilégios. Um exploit de prova de conceito (PoC) foi divulgado, enfatizando a urgência de as organizações aplicarem correções e protegerem seus sistemas para evitar possíveis ataques.

2 DETALHES SOBRE A VULNERABILIDADE

A descrição detalhada da vulnerabilidade é a seguinte:

Natureza da vulnerabilidade

- Vulnerabilidade facilmente explorável que permite que um atacante com privilégios baixos e acesso ao sistema onde o Oracle VM VirtualBox é executado comprometa o Oracle VM VirtualBox.

Impacto

- Ataques bem-sucedidos podem resultar na tomada do controle do Oracle VM VirtualBox.

Pontuação base CVSS 3.1

- **7.8** (impactos de confidencialidade, integridade e disponibilidade).

Vetor CVSS

- (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

Observação

- Essa vulnerabilidade se aplica apenas a hosts Windows.

3 RISCOS PARA AS ORGANIZAÇÕES

Esta vulnerabilidade no Oracle VirtualBox representa riscos significativos para organizações que utilizam essa plataforma de virtualização, incluindo o comprometimento da integridade e confidencialidade. Atacantes podem elevar privilégios em sistemas Windows, acessando ou alterando dados sensíveis. Além disso, podem assumir controle total do VirtualBox, causando paralisações, roubo de dados ou execução de código malicioso. As repercussões de um ataque bem-sucedido incluem grandes custos financeiros, danos à reputação, possíveis violações de regulamentações de segurança e penalidades legais, também pode ser usada como parte de ataques em cadeia, onde um invasor combina várias vulnerabilidades para obter acesso não autorizado a sistemas.

4 RECOMENDAÇÕES

Para proteger suas organizações, é crucial aplicar as atualizações de segurança fornecidas pela Oracle e monitorar atentamente quaisquer atividades suspeitas nos sistemas que executam o Oracle VM VirtualBox.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- NVD
- PoC
- VirtualBox

heimdall
security research
A DIVISION OF ISH