BOLETIM DE SEGURANÇA

Vulnerabilidade do Apache HugeGraph-Server, CVE-2024-27348 sob exploração

heimdall
security research
A DIVISION OF ISH

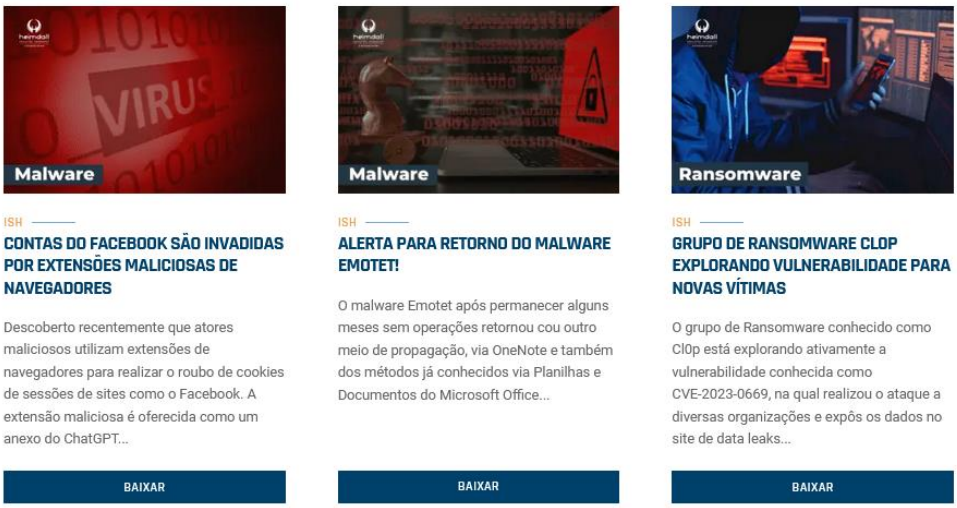
TLP: CLEAR

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 informado pela Shadowserver que a vulnerabilidade do **Apache HugeGraph-Server**, CVE-2024-27348 (CVSS: 9,8) crítica. Provas de conceito (PoC) foram publicadas por pesquisadores de segurança, demonstrando como a vulnerabilidade pode ser explorada.

Figura 1 – Post da Shadowserver em sua página no X.

2 DETALHES SOBRE A VULNERABILIDADE

A falha está localizada na interface do **Gremlin**, a linguagem de travessia utilizada para interagir com o banco de dados gráfico Apache HugeGraph.

Impacto

- Pode levar à execução remota de comandos, possibilitando que um atacante comprometa totalmente o servidor vulnerável.

Versões afetadas

- Apache HugeGraph-Server versões 1.0.0 até antes da 1.3.0 em ambientes Java 8 e Java 11.

Correção

- Atualizar para a versão 1.3.0 e habilitar o sistema de autenticação, o que resolve a vulnerabilidade

Mitigação

- Implementar monitoramento rigoroso para detectar tentativas de exploração desta vulnerabilidade.

3 CONCLUSÃO

Nos últimos anos, vulnerabilidades identificadas em projetos Apache têm se mostrado alvos lucrativos para estados-nação e agentes de ameaças com motivações financeiras. Falhas em componentes como Log4j, ActiveMQ e RocketMQ foram amplamente exploradas para comprometer ambientes específicos. Essas brechas de segurança permitiram invasores acessar sistemas críticos, demonstrando a importância de manter uma postura de segurança proativa e atualizações constantes nos sistemas Apache.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Apache
- Hugegraph
- Shadowserver

heimdall
security research
A DIVISION OF ISH