BOLETIM DE SEGURANÇA

Falha crítica do Bitdefender permite que invasores desencadeiem ataques de falsificação de solicitação do lado do servidor

heimdall
security research
A DIVISION OF ISH

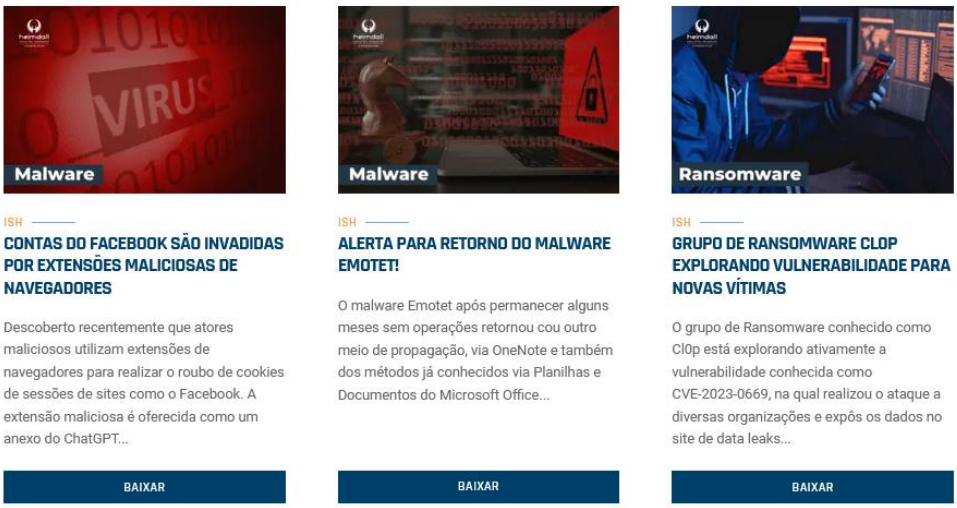
TLP: CLEAR

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 a Bitdefender lançou uma atualização de segurança para correção de uma falha de segurança crítica identificada como **CVE-2024-6980**, e permite que invasores executem ataques de falsificação de solicitação do lado do servidor (SSRF), comprometendo dados e sistemas confidenciais. A análise da pontuação indica que a falha é acessível remotamente (**AV:N**), requer alta complexidade de ataque (**AC:H**) e não requer autenticação (**PR:N**) ou interação do usuário (**UI:N**).

2 DETALHES SOBRE A VULNERABILIDADE

Conforme a Bitdefender a falha é um problema de tratamento de erro verboso no serviço proxy implementado no GravityZone Update Server permite que um invasor cause uma falsificação de solicitação do lado do servidor (SSRF). Essa vulnerabilidade afeta as seguintes versões do GravityZone Console.

- **GravityZone Update Server**, afetado de 0 anterior a 6.38.1-5

Recomendação

- **Atualizar para a versão 6.38.1-5 do produto corrige o problema**

3 SERVIDORES GRAVITYZONE EXPOSTOS NA INTERNET

Em uma busca por servidores GravityZone, foram observados milhares destes expostos na Internet, os quais, estando sem as devidas correções de segurança ou com configurações incorretas, acarretam variados riscos de segurança para os utilizadores.

Figura 1 – Servidores Bitdefender GravityZone expostos na Internet.

4 CONCLUSÃO

As vulnerabilidades no Bitdefender GravityZone têm atraído a atenção de diversos atores de ameaças, que buscam explorar essas falhas para comprometer redes e sistemas. Uma vez comprometido, o sistema pode ser utilizado para movimentos laterais, exfiltração de dados sensíveis e lançamento de ataques adicionais. A importância de manter o Bitdefender GravityZone atualizado e aplicar correções de segurança é crucial para mitigar esses riscos. Além disso, a implementação de uma estratégia de defesa em profundidade, que inclui a monitorização contínua e resposta rápida a incidentes, pode ajudar a proteger as organizações contra essas ameaças.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Bitdefender**
- **Gbhackers**

6 AUTORES

- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH