BOLETIM DE SEGURANÇA

Cisa alerta para três vulnerabilidades sendo exploradas em ataques

heimdall
security research
A DIVISION OF ISH

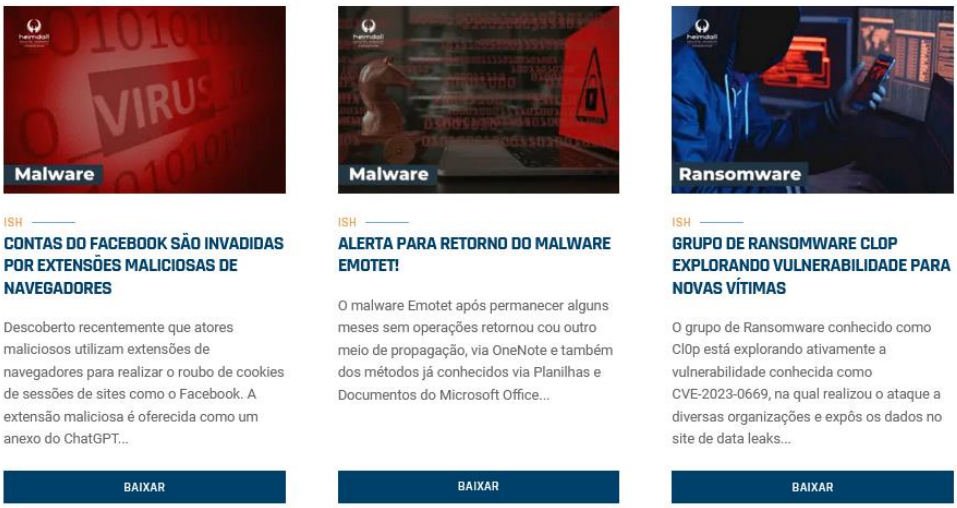
TLP: CLEAR

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

A Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA) adicionou três vulnerabilidades de segurança ao seu catálogo de 'Vulnerabilidades Exploradas Conhecidas' KEV, duas afetando o Google Chrome e uma afetando roteadores D-Link.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

A vulnerabilidade CVE-2024-4761 permite a gravação de dados além dos limites de memória alocados através de uma página HTML maliciosa. Essa falha de segurança tem o potencial de impactar diversos navegadores baseados no Chromium, como Google Chrome, Microsoft Edge e Opera, permitindo a execução de código arbitrário no sistema do usuário.

A vulnerabilidade CVE-2024-4947 afeta o motor V8 do Google Chromium, envolvendo uma confusão de tipos. Essa vulnerabilidade pode ser explorada por um atacante remoto que, ao criar uma página HTML específica, tem a capacidade de executar código arbitrário. Isso representa um risco significativo para os usuários do navegador, pois permite ações mal-intencionadas através da web.

A vulnerabilidade CVE-2021-40655 nos roteadores D-Link DIR-605, é capaz de expor informações sensíveis. Através de uma requisição POST falsificada para a página /getcfg.php, invasores podem adquirir credenciais de usuário e senha. Os produtos afetados são considerados obsoletos pela D-Link, com todas as versões de hardware já no estágio final de vida útil (EOL) ou de serviço (EOS).

3 VULNERABILIDADES ADICIONADAS AO KEV-CISA

Conforme o Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), tais vulnerabilidades são "vetores de ataque frequentes para atores cibernéticos maliciosos".

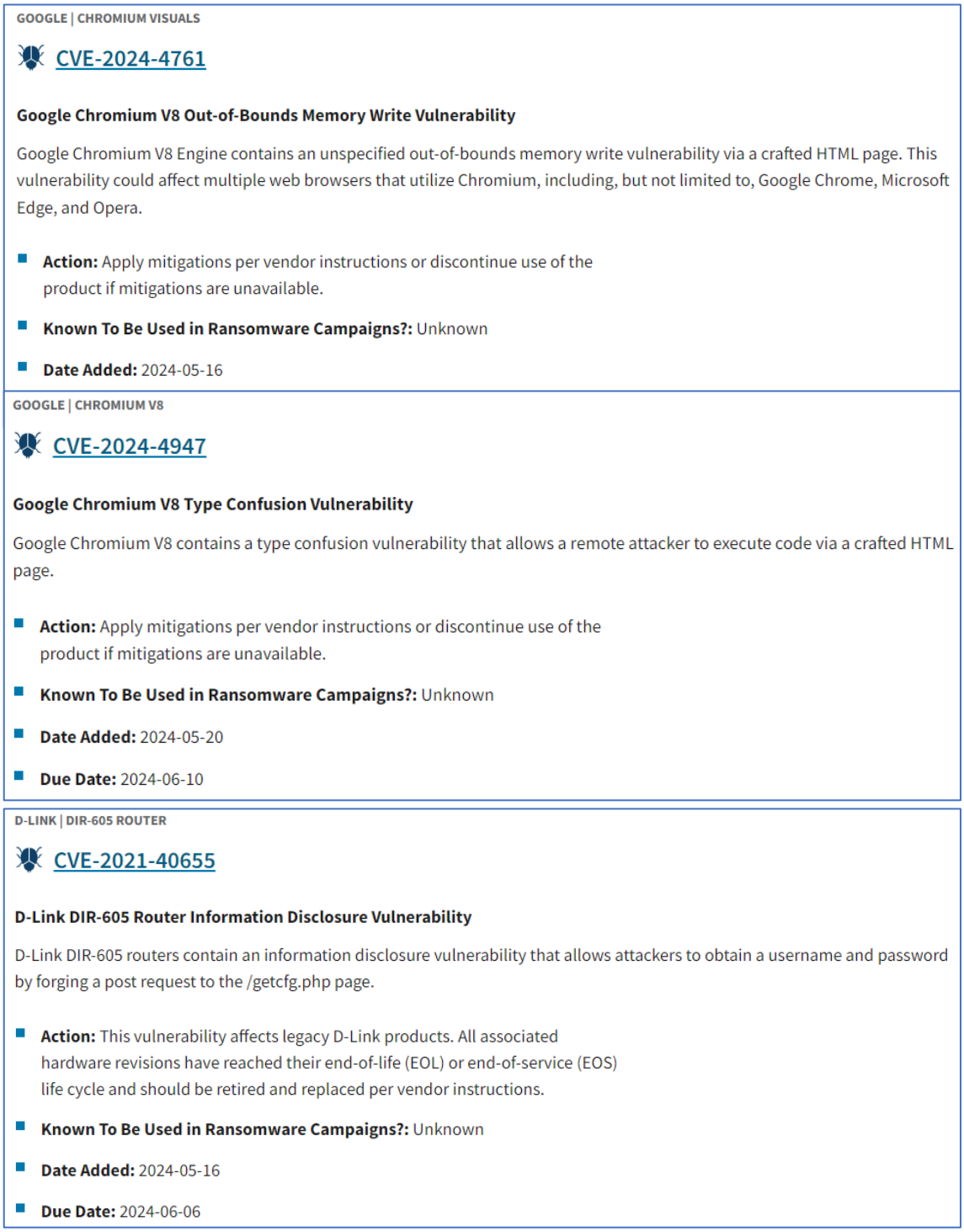


Figura 1 – Vulnerabilidades no catálogo KEV-CISA.

4 RECOMENDAÇÕES

Para as vulnerabilidades CVE-2024-4761 e CVE-2024-4947, recomenda-se atualizar imediatamente para as versões mais recentes do navegador, que são 124.0.6367.207 e 125.0.6422.60, respectivamente. Essas atualizações contêm correções para as falhas de segurança e devem ser aplicadas o quanto antes para evitar explorações maliciosas.

Para CVE-2021-40655, o fabricante informou que os recursos associados a estes produtos cessaram o seu desenvolvimento e já não são suportados e a recomendação é retirar esses produtos e substituí-los por produtos que recebam atualizações de firmware. Além disso, é aconselhável verificar se há boletins de segurança adicionais e aplicar as medidas de mitigação necessárias fornecidas pelo fabricante.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- D-link
- Bleepingcomputer
- CISA_Kev

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH