



BOLETIM DE SEGURANÇA

Google lança correção de segurança para vulnerabilidade
Zero-Day no navegador Chrome



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](#)



ISH —

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH —

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH —

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Sumário Executivo	4
2	Informação sobre a vulnerabilidade	5
3	Recomendações.....	6
4	Referências	7
5	Autores.....	8

1 SUMÁRIO EXECUTIVO

Recentemente a Google implementou atualizações de segurança relacionada a vulnerabilidade [CVE-2024-4671](#) zero-day classificada como críticas que tem como alvo o navegador Chrome. Esta falha específica estava sendo ativamente explorada, conforme reportado pela empresa.

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

A vulnerabilidade **CVE-2024-4671**, foi encontrada no componente visual do Chrome e foi classificada como um erro de uso após liberação. Erros desse tipo ocorrem quando há referências a partes da memória já liberadas, o que pode acarretar desde simples travamentos até a execução de código não autorizado.

Em janeiro, a empresa solucionou um bug que permitia o acesso a áreas de memória não autorizadas no mecanismo V8 do JavaScript e WebAssembly, identificado como CVE-2024-0519, com uma pontuação de gravidade CVSS de 8,8, o que poderia causar falhas no sistema. Além disso, durante o evento Pwn2Own, realizado em março em Vancouver, o Google resolveu mais três vulnerabilidades zero-day, a CVE-2024-2886, que é um erro de uso após liberação encontrado em WebCodecs, a CVE-2024-2887, que se refere a uma confusão de tipos detectada no WebAssembly e a CVE-2024-3159, sendo um problema de acesso à memória fora dos limites no V8.

3 RECOMENDAÇÕES

A Google recomenda que os usuários atualizem para a versão 124.0.6367.201/.202 do Chrome para Windows e macOS e para a versão 124.0.6367.201 para Linux para mitigar ameaças potenciais.

Os usuários de navegadores baseados em Chromium, como Microsoft Edge, Brave, Opera e Vivaldi, também são aconselhados a aplicar as correções conforme e quando estiverem disponíveis.

4 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [Chrome Release](#)
- [Thehackernews](#)
- [Mitre](#)

5 AUTORES

- Leonardo Oliveira Silva



heimdall
security research

A DIVISION OF ISH