



BOLETIM DE SEGURANÇA

Google lança correção para falha zero-day no kernel do
Android explorada em ataques

Acesse a nossa nova comunidade através do
WhatsApp!

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	Introdução executiva.....	5
2	Informações sobre a vulnerabilidade	6
2.1	Sistemas e produtos afetados	6
2.2	Impacto da vulnerabilidade	6
3	Recomendações.....	7
4	Referências	8
5	Autores.....	8

LISTA DE FIGURAS

Figura 1 – Vulnerabilidade CVE-2024-53104 no catálogo KEV-CISA..... 5


1 INTRODUÇÃO EXECUTIVA

O Google divulgou uma vulnerabilidade no kernel do Android, identificada como **CVE-2024-53104**. Esta falha de segurança, já explorada ativamente, permite que agentes mal-intencionados locais autenticados elevem seus privilégios no sistema. A correção foi incluída nas atualizações de segurança de fevereiro de 2025.

LINUX | KERNEL

 [CVE-2024-53104](#) 

Linux Kernel Out-of-Bounds Write Vulnerability: *Linux kernel contains an out-of-bounds write vulnerability in the `uvc_parse_streaming` component of the USB Video Class (UVC) driver that could allow for physical escalation of privilege.*

Related CWE: [CWE-787](#) 

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

■ **Date Added:** 2025-02-05

■ **Due Date:** 2025-02-26

Figura 1 – Vulnerabilidade CVE-2024-53104 no catálogo KEV-CISA.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A [CVE-2024-53104](#) é uma falha de escalonamento de privilégios no driver *USB Video Class (UVC)* do kernel do Android. O problema reside na função *uvc_parse_format*, que não analisa corretamente frames do tipo *UVC_VS_UNDEFINED*. Essa falha resulta em um cálculo incorreto do tamanho do buffer de frames, levando a possíveis gravações fora dos limites da memória. Tais gravações podem ser exploradas para execução arbitrária de código ou ataques de negação de serviço.

As atualizações de segurança do Android de fevereiro de 2025, além de corrigirem um bug de zero-day que estava sendo explorado ativamente, também resolvem uma vulnerabilidade crítica no componente WLAN da Qualcomm. Essa falha, identificada como [CVE-2024-45569](#), é classificada pela Qualcomm como um problema grave de corrupção de memória no firmware. O erro ocorre devido a uma validação inadequada do índice de matriz durante a comunicação do host WLAN, especificamente ao processar o ML IE (Multi-Link Information Element), resultado da presença de um quadro inválido.

2.1 SISTEMAS E PRODUTOS AFETADOS

- Todos os dispositivos que utilizam versões do kernel do Android com o driver UVC vulnerável estão potencialmente em risco.

2.2 IMPACTO DA VULNERABILIDADE

A exploração bem-sucedida desta vulnerabilidade permite que um atacante local autenticado obtenha privilégios elevados no sistema, possibilitando:

- Execução arbitrária de código no contexto do kernel.
- Comprometimento completo do dispositivo afetado.
- Potencial para instalação de malware persistente.
- Acesso não autorizado a dados sensíveis.

3 RECOMENDAÇÕES

Para mitigar os riscos associados a essas vulnerabilidades, é aconselhável:

Aplicar atualização imediata

- Usuários e administradores devem aplicar as [atualizações](#) de segurança de fevereiro de 2025 fornecidas pelo Google ou pelos fabricantes dos dispositivos para corrigir a vulnerabilidade.

4 REFERÊNCIAS

- **Heimdall by ISH Tecnologia**
- [Boletim de segurança do Android](#)
- [Qualcomm](#)
- [Bleeping Computer](#)

5 AUTORES

- **Rafael Salomé**



heimdall
security research

A DIVISION OF ISH