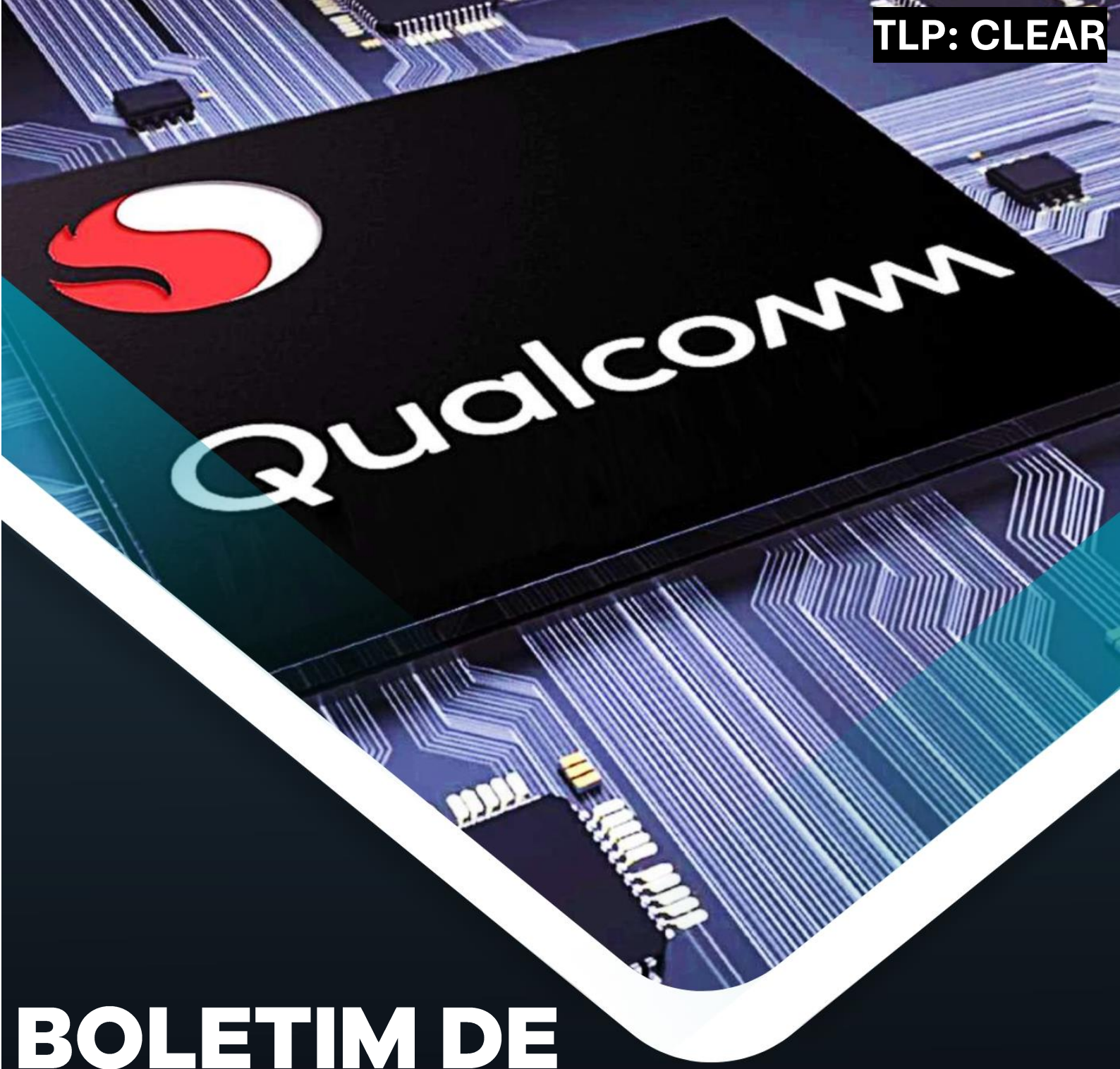
TLP: CLEAR



BOLETIM DE SEGURANÇA

Qualcomm publica patches para vulnerabilidades críticas de dia zero exploradas em ataques

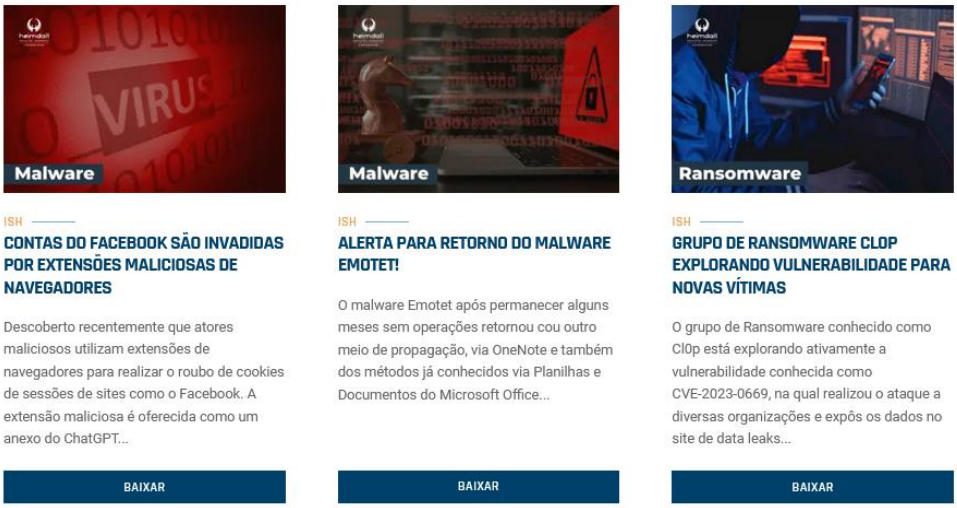
heimdall
security research
A DIVISION OF ISH

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



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A **Qualcomm** lançou atualizações de segurança para corrigir uma vulnerabilidade de *zero day* no Processador de Sinal Digital (DSP), que afeta vários chipsets. A falha, identificada como **CVE-2024-43047** classificada como alta, foi descoberta por pesquisadores do Google Project Zero e do Laboratório de Segurança da Anistia Internacional.

Esta vulnerabilidade pode levar à corrupção de memória quando explorada por invasores com privilégios baixos.

2 DETALHES SOBRE A VULNERABILIDADE

A vulnerabilidade de segurança (CVE-2024-43047) foi identificada por Seth Jenkins, do **Google Project Zero**, e Conghui Wang, do Laboratório de Segurança da Anistia Internacional. Esta falha resulta de uma fraqueza de uso após liberação, que pode causar corrupção de memória quando explorada por invasores locais com privilégios baixos. Atualmente, o DSP atualiza os buffers de cabeçalho com identificadores DMA não utilizados. Na seção **put_args**, se algum identificador DMA estiver presente no buffer de cabeçalho, o mapa correspondente será liberado, conforme descrito em um commit do kernel do DSP.

CVE ID	CVE-2024-43047
Title	Use After Free in DSP Service
Description	Memory corruption while maintaining memory maps of HLOS memory.
Technology Area	DSP Service
Vulnerability Type	CWE-416 Use After Free
Access Vector	Local
Security Rating	High
CVSS Rating	High
CVSS Score	7.8
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Date Reported	2024/07/29
Customer Notified Date	2024/09/02
Affected Chipsets*	FastConnect 6700, FastConnect 6800, FastConnect 6900, FastConnect 7800, QAM8295P, QCA6174A, QCA6391, QCA6426, QCA6436, QCA6574AU, QCA6584AU, QCA6595, QCA6595AU, QCA6688AQ, QCA6696, QCA6698AQ, QCS410, QCS610, QCS6490, Qualcomm® Video Collaboration VC1 Platform, Qualcomm® Video Collaboration VC3 Platform, SA4150P, SA4155P, SA6145P, SA6150P, SA6155P, SA8145P, SA8150P, SA8155P, SA8195P, SA8295P, SD660, SD865 5G, SG4150P, Snapdragon 660 Mobile Platform, Snapdragon 680 4G Mobile Platform, Snapdragon 685 4G Mobile Platform (SM6225-AD), Snapdragon 8 Gen 1 Mobile Platform, Snapdragon 865 5G Mobile Platform, Snapdragon 865+ 5G Mobile Platform (SM8250-AB), Snapdragon 870 5G Mobile Platform (SM8250-AC), Snapdragon 888 5G Mobile Platform, Snapdragon 888+ 5G Mobile Platform (SM8350-AC), Snapdragon Auto 5G Modem-RF, Snapdragon Auto 5G Modem-RF Gen 2, Snapdragon X55 5G Modem-RF System, Snapdragon XR2 5G Platform, SW5100, SW5100P, SXR2130, WCD9335, WCD9341, WCD9370, WCD9375, WCD9380, WCD9385, WCN3950, WCN3980, WCN3988, WCN3990, WSA8810, WSA8815, WSA8830, WSA8835
Patch**	• https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/dsp-kernel/-/commit/0e27b6c7d2bd8d0453e4465ac2ca49a8f8c440e2

Figura 1 – Informações técnicas sobre vulnerabilidade.

No entanto, como o buffer de cabeçalho é acessível a usuários em PD não assinado, eles podem atualizar identificadores inválidos. Se um desses identificadores inválidos corresponder a um já em uso, isso pode resultar em uma vulnerabilidade de use-after-free (**UAF**). A Qualcomm informou que esta vulnerabilidade pode estar sendo explorada de forma limitada e direcionada. Patches para o driver **FASTRPC** foram disponibilizados aos fabricantes de equipamentos originais (OEMs), com uma forte recomendação para que a atualização seja implementada nos dispositivos afetados o mais rápido possível.

Além disso, a Qualcomm corrigiu falhas no chip Snapdragon Digital Signal Processor (DSP), que permitiam a hackers controlar smartphones sem interação do usuário, espionar usuários e criar malware indetectável e irremovível. Outra vulnerabilidade conhecida como **KrØØk**, corrigida em 2020, permitia que invasores descriptografassem pacotes de rede sem fio criptografados com WPA2. Outro bug, agora corrigido, permitia acesso a dados críticos.

3 RECOMENDAÇÕES

A Qualcomm recomenda que os fabricantes de dispositivos implementem as atualizações o mais rápido possível para proteger os usuários.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Qualcomm**
- **Bleepingcomputer**
- **NVD**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH