



# BOLETIM DE SEGURANÇA

ASUS alerta sobre falha grave de autenticação remota  
em sete modelos de roteadores



**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](#)



### 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

---

A ASUS implementou uma atualização de firmware para corrigir uma falha de segurança crítica [CVE-2024-3080](#) que estava presente em sete modelos de seus roteadores, permitindo que invasores remotos acessassem os dispositivos afetados.

## 2 INFORMAÇÃO SOBRE A VULNERABILIDADE

---

A vulnerabilidade CVE-2024-3080 e com uma pontuação CVSS v3.1 de 9,8, foi descoberta em determinados modelos de roteadores da ASUS. Essa falha de segurança permite que invasores remotos não autenticados assumam o controle total do dispositivo. A ASUS confirmou que essa vulnerabilidade afeta especificamente alguns modelos de seus roteadores, como:

- **XT8 (ZenWiFi AX XT8):** Este é um sistema Mesh WiFi 6 tri-band que oferece velocidades de até 6600 Mbps. Ele suporta AiMesh, AiProtection Pro, roaming contínuo e controle dos pais.
- **XT8\_V2 (ZenWiFi AX XT8 V2):** Esta é uma versão atualizada do XT8, que mantém recursos semelhantes, mas com melhorias de desempenho e estabilidade.
- **RT-AX88U:** Este é um roteador WiFi 6 de banda dupla que oferece velocidades de até 6.000 Mbps. Ele vem com 8 portas LAN, AiProtection Pro e QoS adaptável para jogos e streaming.
- **RT-AX58U:** Este é um roteador WiFi 6 de banda dupla que fornece até 3.000 Mbps. Ele suporta AiMesh, AiProtection Pro e MU-MIMO para uma conectividade eficiente de vários dispositivos.
- **RT-AX57:** Este é um roteador WiFi 6 de banda dupla projetado para necessidades básicas, oferecendo até 3.000 Mbps. Ele suporta AiMesh e controles parentais básicos.
- **RT-AC86U:** Este é um roteador WiFi 5 de banda dupla com velocidades de até 2.900 Mbps. Ele vem com AiProtection, QoS adaptativo e aceleração de jogos.
- **RT-AC68U:** Este é um roteador WiFi 5 de banda dupla que oferece até 1900 Mbps. Ele suporta AiMesh, AiProtection e controles parentais robustos.

### 3 RECOMENDAÇÕES

---

A ASUS recomenda que os usuários mantenham seus dispositivos atualizados com as versões mais recentes de firmware, disponíveis para [download](#). Você pode encontrar orientações sobre como atualizar o firmware na página de perguntas frequentes. Se a atualização do firmware não for possível imediatamente, é aconselhável garantir que as senhas da conta e do WiFi sejam seguras, preferencialmente com mais de 10 caracteres não sequenciais.

Adicionalmente, sugere-se que os usuários desativem certos recursos de acesso à Internet, como o painel de administração, acesso remoto de WAN, encaminhamento de porta, DDNS, servidor VPN, DMZ e gatilho de porta.

## 4 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [ASUS](#)
- [Bleepingcomputer](#)
- [NVD](#)

## 5 AUTORES

---

- Leonardo Oliveira Silva



**heimdall**  
security research

A DIVISION OF ISH