



BOLETIM DE SEGURANÇA

CVE-2024-32038, Vulnerabilidade RCE crítica no mecanismo de análise do Wazuh



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	Recomendações.....	5
3	Referências	6

1 SUMÁRIO EXECUTIVO

Recentemente foi descoberta a falha [CVE-2024-32038](#), uma vulnerabilidade crítica de execução remota de código (RCE) que afeta o **Wazuh Manager**, versões de **3.8.0** até **4.7.1**. Esse problema ocorre no componente `wazuh-analysisd`, que é responsável por analisar dados coletados e gerar alertas sobre questões de segurança. A vulnerabilidade se deve a um estouro de buffer ao processar caracteres Unicode provenientes de mensagens do Windows Eventchannel. Um atacante pode explorar essa falha para executar código arbitrário no contexto da conta de serviço do Wazuh Manager.

A gravidade dessa vulnerabilidade é avaliada como crítica, com uma pontuação **CVSS 3.1** de **9.8**, indicando um alto risco de impacto nos aspectos de confidencialidade, integridade e disponibilidade dos sistemas afetados. Não é necessário autenticação para explorar essa vulnerabilidade, e ela pode ser acionada por meio da porta TCP 1514, que é usada por padrão pelo serviço de Analysis Engine.

2 RECOMENDAÇÕES

Para mitigar essa vulnerabilidade, é recomendado atualizar para a versão [4.7.2](#) ou superior do Wazuh Manager, que resolve o problema. Não há soluções alternativas completas, embora limitar os agentes das versões 3.8.0 ou superiores de reportar mensagens do Eventchannel possa ser um paliativo temporário até que a atualização possa ser aplicada.

3 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [Github](#) Wazuh
- [ZeroDayinitiative](#)
- [NVD](#)



heimdall
security research

A DIVISION OF ISH