TLP: CLEAR

Pesquisa de WEB Exploitation

CVE-2025-24016: Execução Remota de Código no Wazuh Server

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse a inteligência que produzimos sobre as Táticas, Técnicas e Procedimentos de determinados *Threat Actors*, análises de *malwares* emergentes no cenário de cibersegurança, análises de vulnerabilidades críticas e outras informações no *blog* da ISH Tecnologia, clicando na imagem abaixo.

ISH

ALERTA HEIMDALL! HTTP2 RAPID RESET_IMPACTOS E DETECÇÃO DA CVE-2023-44487

Falhas de negação de serviço (DoS) não são apenas interrupções técnicas. Elas representam riscos reais à continuidade do negócio, à confiança dos clientes e à reputação da marca. Nisto temos a vulnerabilidade CVE-2023-44487, conhecida como HTTP/2 Rapid Reset.

BAIXAR

ISH

ALERTA HEIMDALL! BABUK2 EM 2025: RETORNO LEGÍTIMO OU COPYCAT ESTRATÉGICO

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, temos o ransomware Babuk2.

BAIXAR

ISH

ALERTA HEIMDALL! A ANATOMIA DO RANSOMWARE AKIRA E SUA EXPANSÃO MULTIPLATAFORMA

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e ganhando bastante popularidade. Nesse contexto, temos o ransomware Akira.

BAIXAR

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1. INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência Heimdall da ISH Tecnologia, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: Estratégico, Tático e Operacional, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2. ESTRATÉGICO

As vulnerabilidades representam condições críticas que podem comprometer a disponibilidade, integridade e confidencialidade de ambientes corporativos. Nesse boletim abordaremos a **CVE-2025-24016**, destacando a importância de sua detecção e mitigação.

2.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

A **CVE-2025-24016** refere-se a uma **falha crítica no Wazuh**, amplamente utilizada para detecção e monitoramento de segurança. A vulnerabilidade pode ser explorada **remotamente por um atacante que possua acesso à API do Wazuh,** permitindo a **execução remota de código** (RCE) no componente vulnerável do servidor Wazuh.

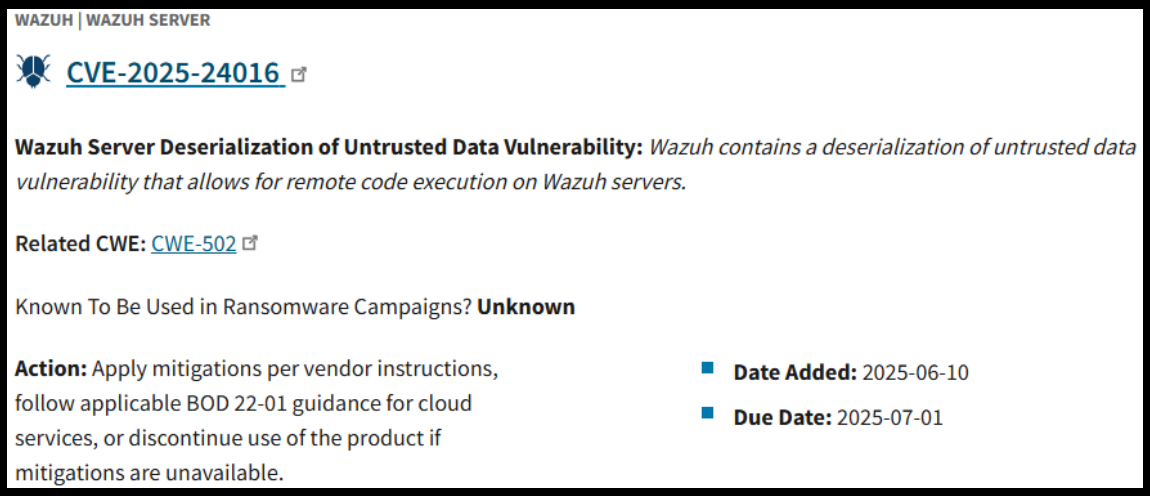

Figura 1- Vulnerabilidade no Catalogo KEV-CISA

A **inclusão da CVE-2025-24016** no catálogo de vulnerabilidades exploradas ativamente ***Known Exploited Vulnerabilities*** **(KEV) da CISA** reforça o entendimento de que a falha **vem sendo explorada em por atores de ameaças**, elevando significativamente o nível de risco associado.

A exploração bem-sucedida dessa falha pode resultar no **comprometimento total do ambiente afetado**, com impacto direto sobre a confidencialidade, integridade e disponibilidade dos sistemas monitorados. Esse elevado potencial de impacto se reflete diretamente no ***Exploit Prediction Scoring System*** (**EPSS**) alto, indicando elevada probabilidade de exploração e forte atratividade da vulnerabilidade para atores de ameaça.

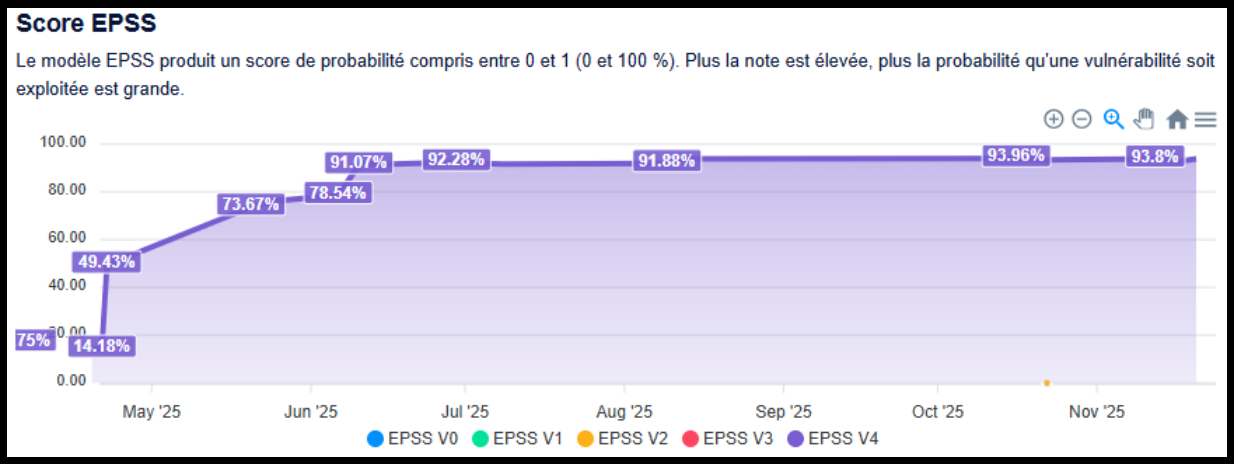

Figura 2- EPSS CVE-2025-24016

2.2 Sistemas, Segmentos e Produtos afetados

Produtos afetados e versões:

- ***Wazuh Server***, nas versões **4.4.0 a 4.9.0**.

Condições de risco adicional:

- Instâncias do **Wazuh *Server*** expostas diretamente à *Internet*;
- Ausência de atualização aplicada de acordo com os comunicados de segurança;
- Configurações que permitam acesso remoto irrestrito aos serviços do *Wazuh Server*;
- Ausência de controles compensatórios, como segmentação de rede, restrições de acesso ou mecanismos de inspeção de tráfego.

Segmentos potencialmente impactados:

- Organizações que utilizam o **Wazuh *Server*** como componente central de monitoramento e correlação de eventos de segurança;
- Provedores de serviços gerenciados (**MSSPs**) que oferecem serviços baseados em **Wazuh** e mantêm instâncias acessíveis remotamente;
- Ambientes corporativos e institucionais que dependem do **Wazuh Server** para a detecção, análise e resposta a incidentes de segurança, onde a exploração da vulnerabilidade pode resultar em **perda de visibilidade, manipulação de alertas e comprometimento da postura defensiva**.

Além dos produtos e segmentos listados, na imagem abaixo podemos observar que o **Wazuh** apresenta ampla distribuição ao redor do mundo.

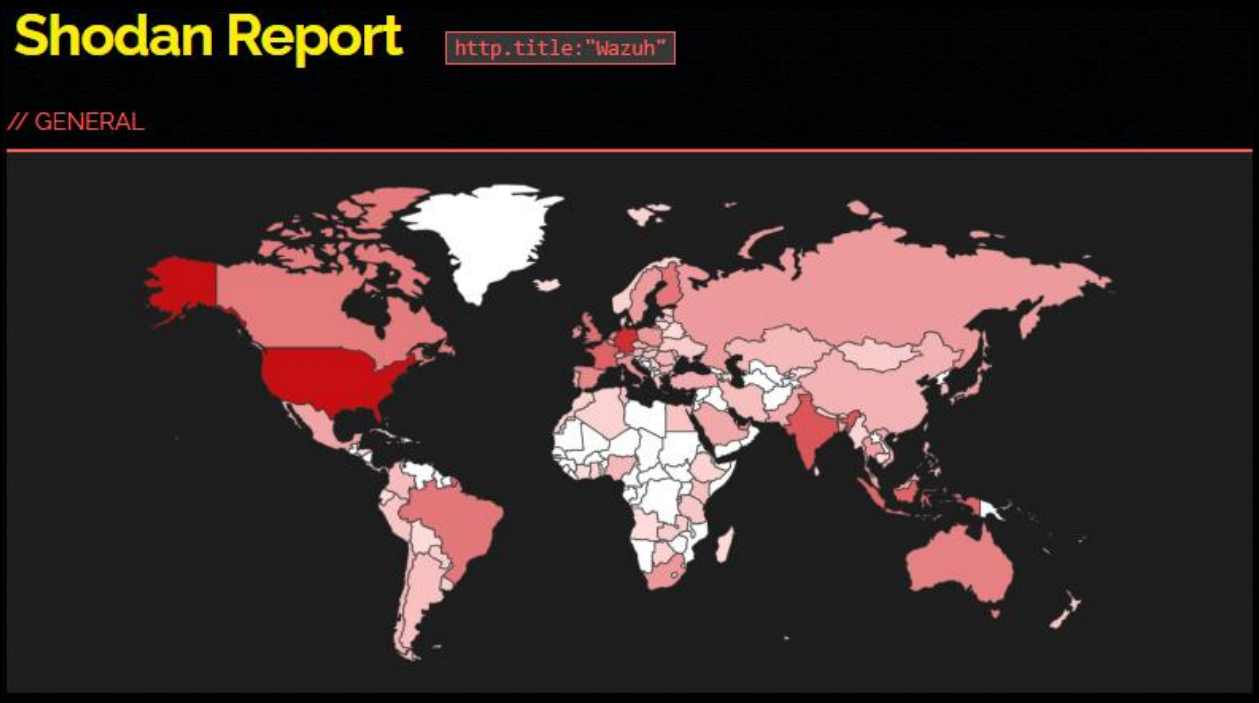

Figura 3 - Distribuição de Dispositivos Expostos (SHODAN)

3. TÁTICO

3.1 Visão geral do Wazuh

O Wazuh é uma plataforma *open source* amplamente utilizada para **monitoramento de segurança, detecção de intrusões, SIEM e XDR**, adotada por organizações de diferentes portes e setores. A solução é composta por múltiplos componentes, sendo o **Wazuh *Server*** responsável pelo processamento, correlação e gerenciamento centralizado dos eventos coletados pelos agentes distribuídos no ambiente.

Entre suas principais funcionalidades estão a análise de *logs*, monitoramento de integridade de arquivos, detecção de ameaças e resposta a incidentes, tornando o **Wazuh** um elemento crítico na arquitetura de defesa de ambientes corporativos. Devido ao seu papel central, o **Wazuh *Server*** normalmente possui **alto nível de privilégio e ampla visibilidade** sobre os ativos monitorados.

Contudo, essa centralização funcional também introduz um **ponto crítico de risco**, uma vez que falhas exploráveis no **Wazuh *Server*** podem permitir que um atacante comprometa não apenas a plataforma de monitoramento, mas também a confiança e a integridade dos mecanismos de detecção de segurança do ambiente.

3.2 Condições para Exploração da Vulnerabilidade

A seguir, são apresentadas as principais condições **indispensáveis** que tornam um ambiente Wazuh vulnerável à exploração da **CVE-2025-24016**:

Condição	Descrição
Uso de versões vulneráveis do Wazuh *Server*	Servidores sem as correções de segurança necessárias.
Disponibilidade da API do Wazuh	A exploração depende do acesso à **API do Wazuh**, que processa requisições contendo dados controlados pelo usuário.
Obtenção de credenciais válidas da API	O atacante precisa possuir **credenciais de um usuário da API do Wazuh** para enviar requisições maliciosas.
Processamento inseguro de *payloads* JSON	A vulnerabilidade é acionada por meio do envio de ***payloads* JSON especialmente manipulados**, explorando um mecanismo inseguro de desserialização.
Ausência de controles compensatórios	Falta de restrições de acesso à **API** que limitem requisições maliciosas.

Tabela 1 - Condição de Exploração

4. OPERACIONAL

4.1 POSSIBILIDADE DE DETEÇÃO

A exploração da **CVE-2025-24016** pode ser identificada por meio da **análise de requisições anômalas direcionadas à API do Wazuh**, utilizando credenciais válidas, mas com ***payloads* JSON maliciosos** projetados para explorar o mecanismo inseguro de desserialização.

Condições

- Tráfego contendo **requisições à API do Wazuh** com estruturas **JSON** incomuns ou campos inesperados, especialmente em *endpoints* que aceitam dados controlados pelo usuário;
- Atividade anômala no **processo do Wazuh *Server***, incluindo a criação de subprocessos inesperados (ex.: ***bash***, ***sh***, ***python***, ***wget***, ***curl***);
- Eventos atípicos nos **logs do Wazuh *Server***, como falhas de processamento, exceções não tratadas ou erros relacionados à desserialização;
- **Correlação de eventos no próprio Wazuh**, associando chamadas à **API** com comportamentos suspeitos observados no *host* onde o Wazuh *Server* está em execução.

4.2 MITIGAÇÃO

A mitigação deve priorizar a **aplicação imediata das correções disponibilizadas pelo fornecedor**, bem como a **restrição do acesso à API do Wazuh**, reduzindo a superfície de ataque exposta.

Correção imediata

- Atualizar o **Wazuh *Server* para versão corrigida**, conforme orientação oficial do projeto Wazuh;
- Restringir o acesso à **API do Wazuh** apenas a redes internas ou endereços IP confiáveis;
- Revisar e limitar as **credenciais da API**, garantindo o princípio do menor privilégio e removendo acessos desnecessários.

Mitigação compensatória (temporária)

- Implementar regras em ***firewalls*, WAFs ou IDS/IPS** para limitar ou inspecionar requisições à API do Wazuh;
- Aplicar segmentação de rede para isolar o Wazuh *Server* de acessos externos diretos;
- Intensificar o monitoramento de chamadas à API e da execução de processos no *host* até a aplicação definitiva da correção.

5. CONCLUSÃO

O Wazuh é uma plataforma de segurança amplamente adotada para monitoramento, correlação de eventos e resposta a incidentes. A **CVE-2025-24016** evidencia a criticidade de vulnerabilidades **nessa solução**, especialmente quando componentes centrais, como o **Wazuh *Server***, estão expostos ou acessíveis a partir de redes externas. O rápido crescimento na probabilidade de exploração da vulnerabilidade, junto com a **inclusão da CVE-2025-24016** no catálogo **KEV da CISA** reforça esse amadurecimento do cenário de exploração e indica sua adoção progressiva por atores de ameaça.

A aplicação imediata das correções disponibilizadas pelo fornecedor, aliada à **restrição de acesso à API do Wazuh** e à revisão de credenciais e permissões, é fundamental para reduzir o risco de comprometimento. O uso adequado das capacidades nativas do próprio Wazuh para **monitoramento e correlação de eventos** complementa a postura defensiva, permitindo identificar tentativas de exploração e atividades suspeitas de forma mais ágil.

Mais do que um caso isolado, a CVE-2025-24016 reforça a importância de **práticas consistentes de gestão de vulnerabilidades**, controle de exposição de interfaces críticas e *hardening* de soluções de segurança, evitando que falhas conhecidas evoluam para vetores recorrentes de comprometimento em ambientes corporativos.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- **NIST**
- **CVEFIND**
- **SHODAN**
- **CISA-KEV**

AUTORES

Gustavo Jatene de Oliveira - Security Researcher

heimdall
security research
A DIVISION OF ISH