TLP: CLEAR

Pesquisa de WEB Exploitation

CVE-2025-48703: RCE no CentOS Web Panel (CWP)

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 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

A vulnerabilidade citada representa condições críticas que podem comprometer a disponibilidade, integridade e confidencialidade de ambientes corporativos. Nesta seção, destacamos a CVE-2025-48703.

2.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

A CVE-2025-48703 refere-se a uma falha crítica **(CVSSv3 de 9.0)** de segurança no **CentOS Web Panel (CWP)**. A vulnerabilidade pode ser explorada remotamente e sem necessidade de autenticação, permitindo a execução arbitrária de comandos no servidor vulnerável. A exploração dessa falha pode resultar em impacto direto sobre a **confidencialidade, integridade** e **disponibilidade** de sistemas expostos à *internet*.

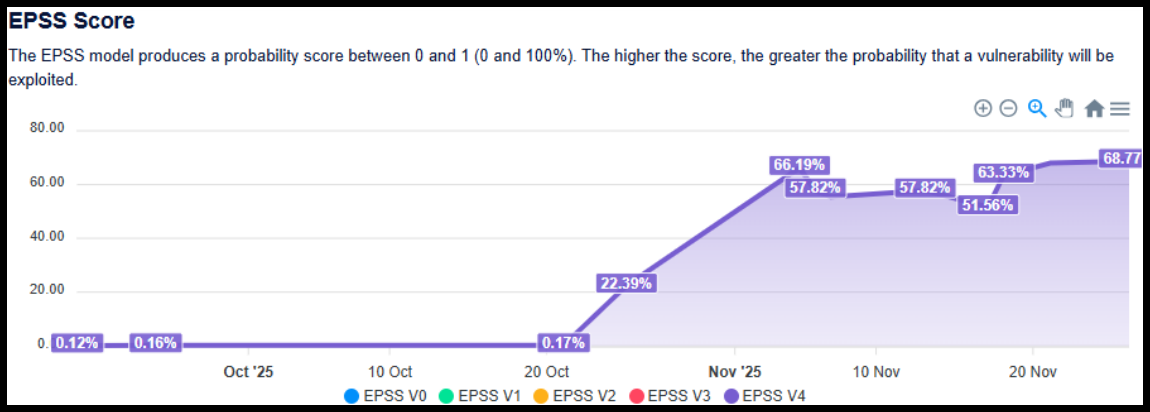

Figura 1- Histórico de EPSS da CVE-2025-48703

A inclusão da CVE nos alertas de vulnerabilidades exploradas ***Known Exploited Vulnerabilities*** **(KEV)** da **CISA** reforça a preocupação de que está sendo utilizada ativamente em campanhas maliciosas. Paralelamente, observa-se um aumento significativo na pontuação do ***Exploit Prediction Scoring System*** **(EPSS)** da **CVE-2025-48703**, conforme ilustrado na imagem abaixo.

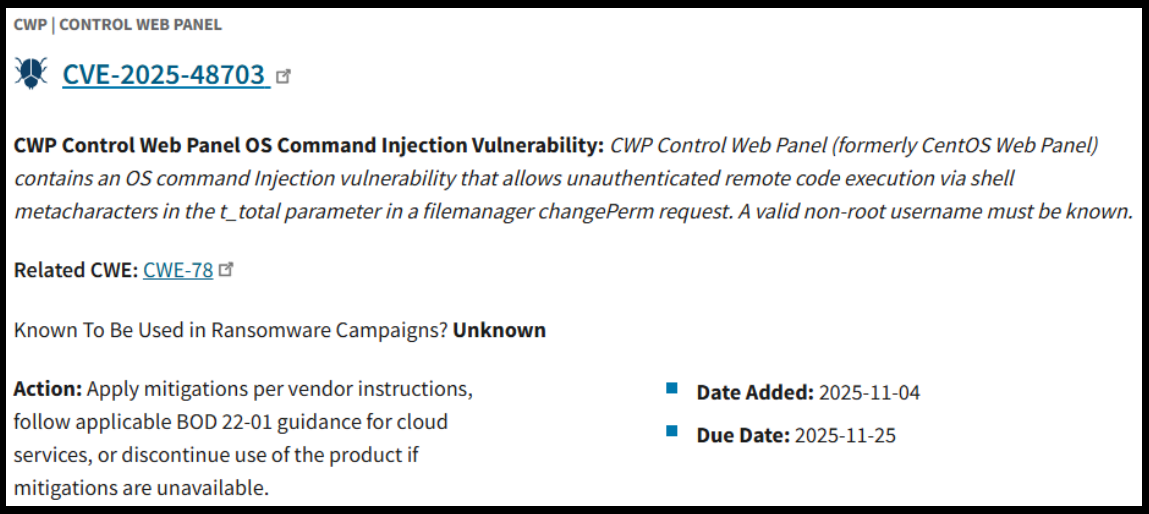

Figura 2- CVE-2025-48703 no catálogo KEV-CISA

Esses indicadores demonstram que a vulnerabilidade está se tornando progressivamente mais suscetível à exploração por atores de ameaça.

2.2 Sistemas, Segmentos e Produtos afetados

Produtos afetados e versões:

- Versões abaixo de **0.9.8.1204**.

Condições de risco adicional:

- Instâncias do ***CentOS Web Panel*** expostas diretamente à *Internet*;
- Ausência de atualização aplicada de acordo com os comunicados de segurança;
- Falta de mecanismos de defesa como **WAFs** (***Web Application Firewalls***) ou configurações de segurança que limitem o acesso remoto;

Segmentos potencialmente impactados:

- **Provedores de hospedagem** e empresas que utilizam ***CentOS Web Panel*** para **gerenciar múltiplos servidores** de clientes, onde a falha pode permitir a execução remota de comandos no sistema afetado;
- **Organizações** que utilizam ***CentOS Web Panel*** para **gerenciar infraestruturas críticas**, como servidores de **e-commerce**, **SaaS** ou **financeiros**, onde a exploração da vulnerabilidade pode resultar em comprometimento de dados sensíveis ou interrupção de serviços.

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

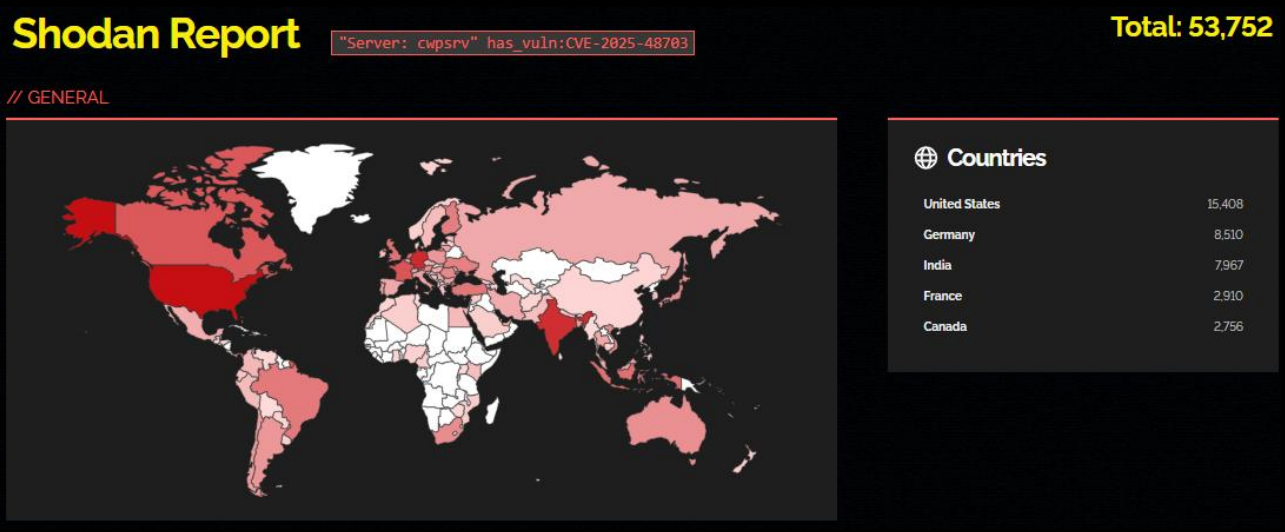

Figura 3- Dispositivos expostos (SHODAN)

Um outro ponto evidenciado na imagem é a quantidade expressiva de dispositivos potencialmente vulneráveis expostos à *Internet*.

3. TÁTICO

3.1 VISÃO GERAL DO CWP

O ***CentOS Web Panel*** **(CWP)** é uma ferramenta de administração voltada para servidores **Linux**, amplamente utilizada por provedores de hospedagem e administradores de sistemas. Ele permite gerenciar, por meio de uma *interface web*, diversos serviços essenciais, como **Apache**, **MySQL**, **e-mail**, **DNS** e contas de usuários.

Sua arquitetura integra componentes *web* e *scripts* de *backend* que executam comandos administrativos diretamente no sistema, oferecendo grande flexibilidade, mas também ampliando a superfície de ataque quando exposto à *Internet*.

Em ambientes de produção, especialmente aqueles com múltiplos domínios ou usuários, o CWP desempenha um papel crítico na gestão da infraestrutura. Por isso, a correta configuração, o controle de acesso ao painel e a aplicação regular de atualizações são medidas fundamentais para garantir a segurança da plataforma.

4. OPERACIONAL

4.1 POSSIBILIDADE DE DETEÇÃO

A exploração da CVE-2025-48703 pode ser identificada por meio das requisições anômalas não autenticada, explorando a manipulação de parâmetros em *endpoints* administrativos.

Condições

- **Tráfego** contendo requisições **POST** ou **GET** direcionadas à *interface* de administração do **CWP**, com parâmetros anômalos que possam indicar injeção de comandos;
- Atividade anômala do processo da aplicação, com criação de subprocessos inesperados (ex.: **bash**, **sh**, **wget**, **curl** etc.);
- Monitorar os **logs** do **CWP**, preferencialmente encaminhando-os ao **SIEM** para análise contínua e correlação com indicadores de exploração.

4.2 MITIGAÇÃO

A mitigação deve priorizar a aplicação imediata da atualização disponibilizada pelo fornecedor e a redução da superfície de exposição da *interface* de administração.

Correção imediata

- Aplicar a **versão 0.9.8.1204 ou superior** do ***CentOS Web Panel***, conforme comunicado oficial;
- Restringir o acesso à *interface* administrativa apenas a endereços internos ou redes de gestão confiáveis;
- Habilitar autenticação de **multifator** (se aplicável) e revisar permissões do painel.

Mitigação compensatória (temporária)

- Implementar regras de inspeção em **WAFs** ou **IDS/IPS** para bloquear requisições contendo **padrões de execução remota**;

5. CONCLUSÃO

A **CVE-2025-48703** destaca a criticidade de vulnerabilidades em soluções amplamente empregadas para administração de servidores, especialmente quando expostas à *Internet*. Embora tenha sido divulgada recentemente, em **setembro de 2025**, a falha rapidamente ganhou espaço em campanhas ativas, refletindo o alto interesse de agentes maliciosos nesse vetor. A inclusão no catálogo **KEV da CISA** reforça essa tendência e evidencia a necessidade de atenção imediata por parte das organizações que utilizam o **CentOS Web Panel (CWP).** A correção imediata, aliada à restrição de acesso administrativo e ao uso de controles adicionais de proteção, é essencial para reduzir o risco de comprometimento. O monitoramento contínuo de tentativas de exploração e atividades pós-comprometimento complementa a resposta defensiva, permitindo identificar e conter incidentes de forma ágil.

Mais do que um caso isolado, a **CVE-2025-48703** reforça a importância de práticas consistentes de **gestão de vulnerabilidades** e ***hardening* de serviços expostos**, prevenindo que falhas recém-divulgadas sejam rapidamente exploradas em larga escala.

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