

TLP: CLEAR



Pesquisa de WEB Exploitation

Exploração ativa: CVE-2025-25257- Ameaça
Segurança de Aplicações Web

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!



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

1. INTRODUÇÃO EXECUTIVA.....	5
2. ESTRATÉGICO	5
2.1 Introdução sobre a vulnerabilidade	5
2.2 Sistemas, Segmentos e Produtos afetados.....	6
3. TÁTICO	7
3.1 Utilização da CVE-2025-25257 em campanhas	7
4. OPERACIONAL.....	7
4.1 Possibilidade de detecção	7
4.2 Mitigação.....	7
5. CONCLUSÃO	8
Referências	9
Autores	9

LISTA DE FIGURAS

Figura 1 - EPSS CVE-2025-25257	5
Figura 2 - CVE-2025-25257 no catalogo KEV-CISA.....	6
Figura 3 - Distribuição do uso da CVE-2025-25257	7

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 identificada representa uma condição crítica que pode comprometer a **disponibilidade**, **integridade** e **confidencialidade** dos ambientes corporativos. Nesta seção, destacamos a **CVE-2025-25257**, cuja exploração potencial configura um risco estratégico relevante para a segurança da informação.

2.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

A **CVE-2025-25257** refere-se a uma falha crítica (**CVSSv3 de 9.8**) de segurança no **FortiWeb**. A vulnerabilidade pode ser explorada remotamente e sem necessidade de autenticação, permitindo que atores de ameaça façam consultas **SQL** maliciosas, podendo manipular os dados armazenados no banco de dados. A exploração dessa falha pode resultar em impacto direto sobre a **confidencialidade**, **integridade** e **disponibilidade** de sistemas expostos à *internet*.

Em observação do **Exploit Prediction Scoring System (EPSS)** da **CVE-2025-25257**, podemos notar a constância em sua probabilidade de uso, e mesmo que o índice não seja considerado extremamente elevado, ele também não pode ser classificado como irrelevante. A vulnerabilidade já foi incluída no **Known Exploited Vulnerabilities (KEV)** da **CISA**, confirmando que está sendo utilizada em campanhas por atores de ameaça, entretanto, ainda não há evidências de exploração atribuída a grupos de *ransomware*.



Figura 1 - EPSS CVE-2025-25257

FORTINET | FORTIWEB

[CVE-2025-25257](#)

Fortinet FortiWeb SQL Injection Vulnerability: Fortinet FortiWeb contains a SQL injection vulnerability that may allow an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPS requests.

Related CWE: [CWE-89](#)

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

■ **Date Added:** 2025-07-18

■ **Due Date:** 2025-08-08

Figura 2 - CVE-2025-25257 no catalogo KEV-CISA

2.2 SISTEMAS, SEGMENTOS E PRODUTOS AFETADOS

Produtos afetados e versões:

- FortiWeb 7.6.0 até 7.6.3;
- FortiWeb 7.4.0 até 7.4.7;
- FortiWeb 7.2.0 até 7.2.10;
- Versões abaixo de 7.0.10.

Condições de risco adicional:

- **Instâncias FortiWeb expostas** diretamente à Internet (consoles de gestão ou endpoints de administração);
- Ausência de atualização aplicada de acordo com os comunicados do fornecedor;
- Falta de mecanismos de *virtual patching* ou assinaturas **IPS** que detectem padrões de **SQLi**;
- **Logs** e monitoramento insuficientes para identificar requisições malformadas ou comandos **SQL** anômalos;

Segmentos potencialmente impactados:

- **Operadoras e provedores de serviços** que usam FortiWeb para proteger aplicações de clientes;
- **Empresas que usam FortiWeb como primeira linha de defesa para aplicações críticas** (financeiro, e-commerce, SaaS), onde a falha pode levar à exposição de dados sensíveis;
- **Pequenas e médias empresas (PMEs)** que podem atrasar atualizações ou não aplicar mitigação compensatória.

3. TÁTICO

3.1 UTILIZAÇÃO DA CVE-2025-25257 EM CAMPANHAS

Após a divulgação da PoC da **CVE-2025-25257**, observou-se um crescimento exponencial nas tentativas de exploração da vulnerabilidade, possivelmente sugerindo que sejam ataques automatizados e/ou varreduras em massa. Até o momento das publicações oficiais/relatos públicos consultados, não há ampla atribuição pública a grupos APT específicos.

Ainda que não haja atribuição pública a grupos APT, com os dados disponíveis podemos observar o uso ativo da CVE-2025-25257. A imagem abaixo mostram tentativas de exploração em diferentes regiões no último mês, indicando que a falha segue sendo visada.

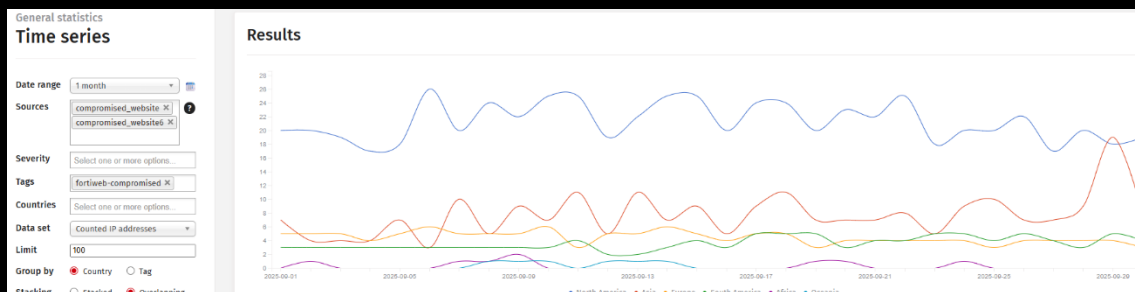


Figura 3 - Distribuição do uso da CVE-2025-25257

4. OPERACIONAL

4.1 POSSIBILIDADE DE DETECÇÃO

A exploração da **CVE-2025-25257** pode ser identificada por meio de sinais em pontos específicos dado que o vetor inicial é uma **injeção SQL não autenticada** em **endpoints HTTP/HTTPS** do FortiWeb.

Condições

- **Tráfego HTTP/HTTPS:** Requisições POST/GET com padrões de SQLi direcionadas à interface de gestão do FortiWeb;
- **Processo:** Atividade anômala no processo httpsd.

4.2 MITIGAÇÃO

A mitigação deve priorizar **aplicação imediata de patches** e redução da exposição das interfaces de gestão.

Correção imediata

- Aplicar os *patches* oficiais do **Fortinet**;
- Se a atualização não for possível, restringir o acesso à *interface* de gestão (**ACLs**, **VPN**, *jump hosts* ou segmentação de rede).

Mitigação compensatória (temporária)

- Aplicar regras de inspeção (em **firewalls/IPS**) para bloquear tentativas de **SQLi** direcionadas à *interface* administrativa, **se aplicável**;
- Garantir que *logs* detalhados (**httpsd**, **CGI**) estejam habilitados e sendo enviados ao **SIEM**.

5. CONCLUSÃO

A exploração da **CVE-2025-25257** representa uma ameaça crítica, com potencial para comprometer diretamente dispositivos **FortiWeb** expostos. A rápida utilização da falha após a divulgação da **PoC** reforça o interesse recorrente desses ativos por agentes maliciosos, especialmente quando expostos à *internet*.

Do ponto de vista defensivo, é fundamental reduzir a superfície de ataque, aplicando *patches* oficiais da **Fortinet**, restringir o acesso às interfaces de gestão e adotar segmentação de rede. Adicionalmente, mecanismos de detecção e resposta devem monitorar tentativas de **injeção SQL** nas *interfaces web* e ações pós-comprometimento, como criação de *webshells* e alteração de contas administrativas, permitindo contenção ágil e eficaz. A **CVE-2025-25257** não deve ser tratada como um caso isolado, mas como parte de um cenário mais amplo em que falhas em *appliances* de segurança expostos podem se tornar vetores críticos de ataque. Isso reforça a necessidade de uma abordagem contínua de gestão de vulnerabilidades, monitoramento proativo e aplicação de práticas de *hardening* em ambientes sensíveis.

REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- CTI Purple Team *by* ISH Tecnologia
- [NIST](#)
- [CVEFIND](#)
- [SECURITY AFFAIRS](#)
- [SHADOWSERVER](#)
- [CISA-KEY](#)

AUTORES

Gustavo Jatene de Oliveira – Security Researcher



heimdall
security research

A DIVISION OF ISH