TLP: CLEAR

RELATÓRIO DE PESQUISAS

“Ni8mare” – Análise da CVE-2026-21858

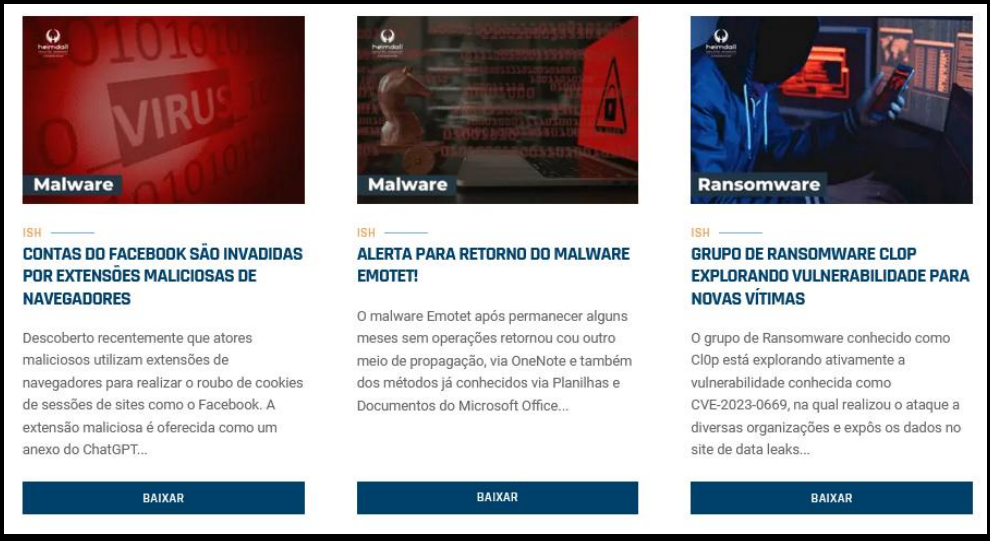
heimdall
security research
A DIVISION OF ISH

Acesse a nossa nova comunidade através do WhatsApp!

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



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência **CTI-Purple Team 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

2.1 INTRODUÇÃO SOBRE A AMEAÇA

A CVE-2026-21858 é uma falha de ***Directory Traversal*** (Travessia de Diretório) que afeta o software de automação de fluxo de trabalho **n8n** em **versões anteriores à 1.76.0.**

A vulnerabilidade reside no componente **formidable (v2.1.2)**, utilizado para processar uploads. Devido a uma validação insuficiente de cabeçalhos ***Content-Disposition***, um atacante pode escapar do diretório de upload e ler arquivos sensíveis do sistema operacional ou injetar configurações maliciosas, resultando em Execução Remota de Código (RCE).

2.2 ÍNDICES E TELEMETRIA EPSS

A análise temporal do ***EPSS*** *(Exploit Prediction Scoring System)* evidencia o momento exato da "armatização" da vulnerabilidade.

Conforme demonstrado no gráfico abaixo, a probabilidade de exploração sofreu um **salto vertical em 12 de janeiro**, saindo de índices residuais (0.03%) para exploração ativa em menos de 24 horas. Atualmente, a vulnerabilidade encontra-se no **percentil 89%,** o que significa que ela apresenta um risco de exploração superior à vasta maioria das vulnerabilidades catalogadas mundialmente.

Este comportamento gráfico (ascensão rápida e sustentada) é característico de vulnerabilidades que foram rapidamente adotadas por grupos de *Ransomware* e *Botnets* após a divulgação de códigos de exploração pública (PoCs). Até o momento de confecção desta pesquisa, não foi atrelado nenhum grupo ou campanha a vulnerabilidade.

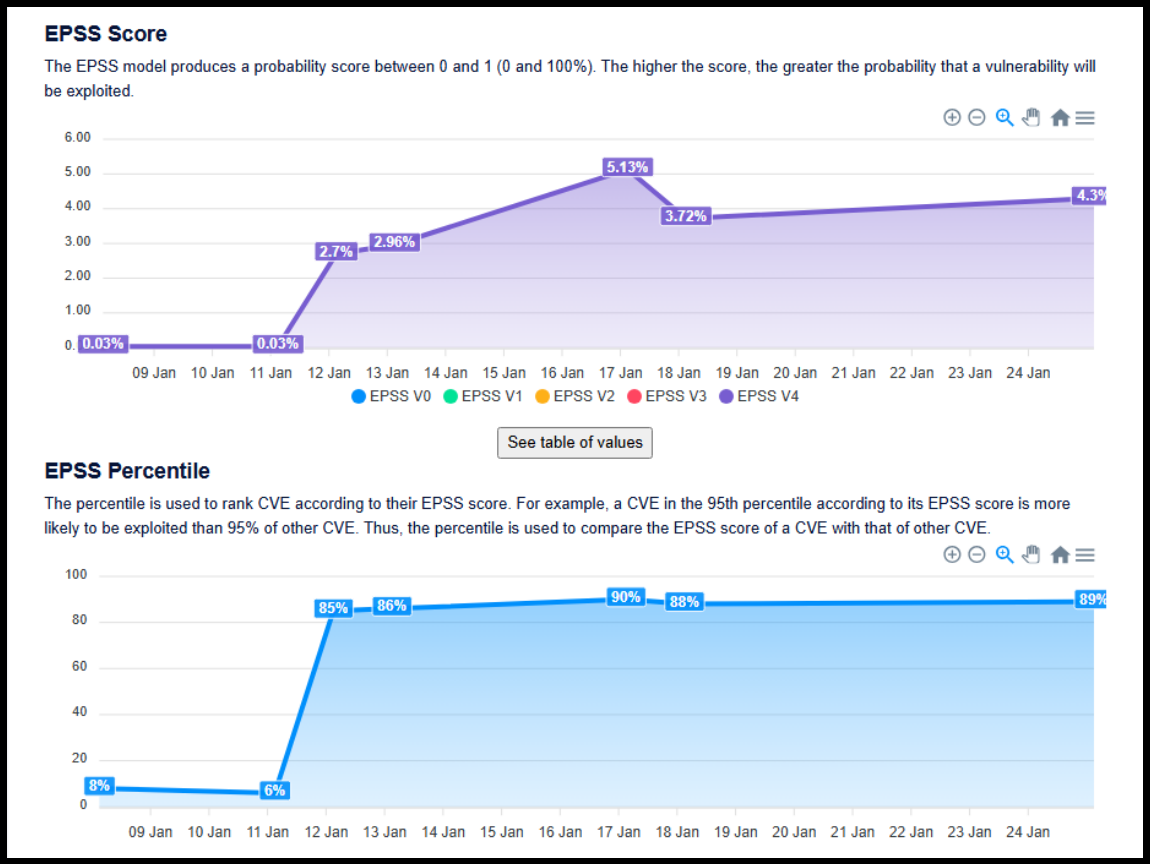


Figura 1- EPSS Score & EPSS Percentile

2.3 VITIMOLOGIA E ATAQUE

O impacto estratégico deriva da função do n8n como um "**Cofre de Credenciais**". A ferramenta centraliza chaves de API críticas (AWS, GCP, OpenAI, Stripe) para integrar serviços. O comprometimento de uma instância concede ao atacante acesso lateral a toda a pilha tecnológica da vítima.

Os alvos primários identificados incluem:

- **Startups de IA/ML:** Usuários intensivos de APIs expondo webhooks publicamente para integração rápida
- **Equipes de DevOps:** Automação CI/CD com portas públicas (5678) para hooks do GitHub/GitLab
- **Automação de Marketing:** Integrações de CRM e analytics com exposição direta à internet.

A distribuição geográfica das instâncias vulneráveis revela concentrações críticas em regiões estratégicas. O mapa de calor abaixo demonstra a densidade de exposição global, com tonalidades mais escuras indicando maior concentração de alvos potenciais. Notavelmente, as regiões de alta densidade (América do Norte, Europa Ocidental e Ásia-Pacífico) também correspondem às áreas com

maior atividade de threat actors conhecidos, aumentando exponencialmente o risco de exploração em massa.

Figura 2 - Distribuição Global do n8n (shodan)

3 TÁTICO

3.1 O QUE É O N8N ?

O **n8n** é uma plataforma de **automação de fluxo de trabalho** (*workflow automation*) "*source-available*", amplamente adotada por equipes de Engenharia, DevOps e Startups de IA para orquestrar integrações complexas. Diferente de concorrentes SaaS (como Zapier), o n8n é projetado para ser **auto-hospedado** (*self-hosted*), permitindo que empresas processem dados sensíveis dentro de sua própria infraestrutura.

Do ponto de vista ofensivo, o n8n não é apenas um executor de tarefas, mas um **Cofre de Credenciais Ativo**. Para realizar integrações entre serviços, a plataforma precisa armazenar e descriptografar em tempo de execução:

- Chaves de acesso à Nuvem (AWS Access Keys, Google Service Accounts);
- Tokens de API de terceiros (OpenAI, Stripe, Slack);
- Credenciais de Banco de Dados (PostgreSQL, MySQL, Redis).

Essa característica arquitetural torna o n8n um "Ponto Único de Falha" (*Single Point of Failure*): comprometer uma instância significa, invariavelmente, obter acesso lateral a toda a pilha tecnológica conectada a ela.

A imagem abaixo exemplifica como esses fluxos de trabalho são estruturados.

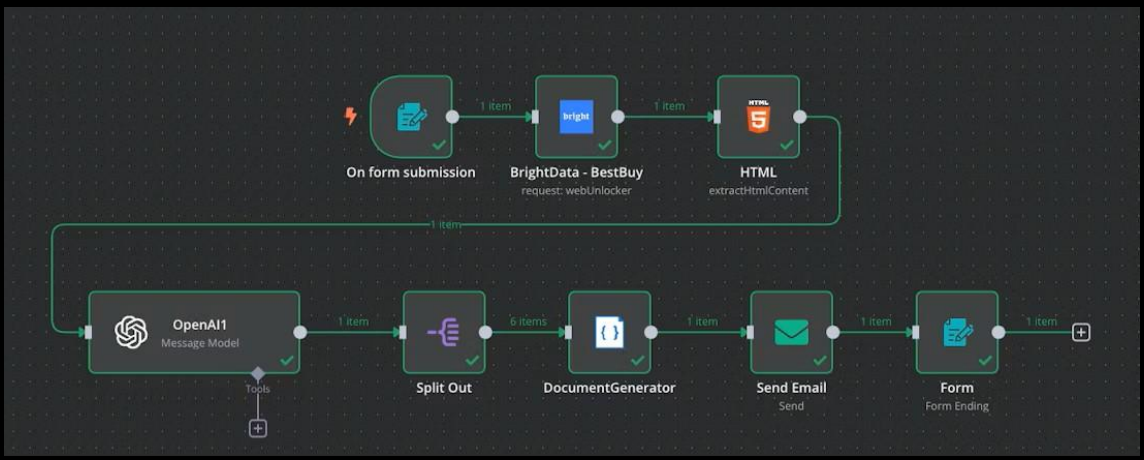


Figura 3 - Fluxo n8n

3.2 Mapeamento e Modus Operandi

A exploração baseia-se em uma técnica de **"Confusão de Tipo"** (*Type Confusion*).

- **O Gatilho:** Requisições application/json passam por verificações de autenticação rigorosas. No entanto, requisições multipart/form-data (usadas para uploads) invocam o parser vulnerável formidable antes da validação completa de segurança.
- **Evasão:** Atacantes camuflam o tráfego malicioso como uploads de arquivos legítimos, contornando WAFs baseados em assinatura que não inspecionam a profundidade dos nomes de arquivo em formulários multipart.

4 Operacional

4.1 Sequência de Exploração (Kill Chain)

A cadeia de ataque segue três estágios distintos e documentados:

1. **Exfiltração de Banco de Dados:** O atacante envia uma requisição manipulada contendo o caminho **../../../../home/node/.n8n/database.sqlite** no campo *filename*. O servidor devolve o banco de dados contendo credenciais e sessões.
2. **Decriptografia de Segredos:** Utilizando uma segunda requisição para roubar o arquivo .env (onde reside a N8N_ENCRYPTION_KEY), o atacante descriptografa as credenciais (AES-256-CBC) offline.
3. **Persistência e RCE:** Com acesso administrativo, o atacante estabelece persistência via **Shadow Admin** (inserção direta de usuário no banco SQLite) ou cria **Cron Workflows** (tarefas agendadas) que executam *reverse shells* a cada 6 horas para manter o acesso.

4.2 Recomendações e Mitigação

A ação corretiva deve ser imediata incluir os itens abaixo:

- **Patch Emergencial:** Atualizar para a versão **1.76.0** ou superior, que implementa a normalização estrita de caminhos (path.basename).
- **Rotação Total de Credenciais:** Devido à natureza da falha (vazamento do banco de dados), **todas** as chaves de API e senhas armazenadas no n8n devem ser revogadas e rotacionadas. Apenas atualizar o software não remove o risco de credenciais já roubadas.
- **Isolamento de Rede:** Remover a exposição pública da porta 5678. O acesso ao painel de gerenciamento deve ser restrito via VPN ou Túnel autenticado.

4.3 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Initial Access	**T1190**	Exploração de aplicação pública via *Path Traversal*.
Credential Access	**T1555.005**	Extração de credenciais de arquivos de configuração e bancos de dados locais.
Persistence	**T1053.003**	Uso de tarefas agendadas (Cron Workflows) dentro da aplicação para manter acesso.
Defense Evasion	**T1036.005**	Mascaramento de *workflows* maliciosos com nomes legítimos (ex: "System Health Monitor").

Tabela 1 – Tabela MITRE ATT&CK.

5 Conclusão

A **CVE-2026-21858 (Ni8mare)** exemplifica o risco extremo de vulnerabilidades em plataformas de orquestração "*Low-Code*". A combinação de facilidade de exploração (pré-autenticação) com o alto valor dos ativos comprometidos (chaves de nuvem e dados de produção) exige uma postura de defesa em profundidade, indo além do *patching* e focando na segmentação de rede e gestão de segredos.

6 Referências

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- CveFind
- SentinelOne Blog
- CisoAdvisor

7 Autores

Lucas Andrade Silva – CyberSecurity Researcher

heimdall
security research
A DIVISION OF ISH