

The image shows the word 'NextJS' in a 3D, metallic, glowing blue font. The letters are raised and have a bright blue light emanating from their base, creating a strong glow effect. The text is set against a dark, reflective surface that appears to be part of a device or a futuristic interface, with some faint lines and a small blue dot visible in the background.

RELATÓRIO DE PESQUISAS

WEB Exploitation

CVE-2025-29927: Exploração via Header em Next.js






heimdall
security research

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.

| | | |
|---|--|---|
|  Malware |  Malware |  Ransomware |
| <p>ISH</p> <p>CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES</p> <p>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...</p> <p>BAIXAR</p> | <p>ISH</p> <p>ALERTA PARA RETORNO DO MALWARE EMOTET!</p> <p>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...</p> <p>BAIXAR</p> | <p>ISH</p> <p>GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS</p> <p>O grupo de Ransomware conhecido como Cl0p 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...</p> <p>BAIXAR</p> |

SUMÁRIO

| | |
|---|----|
| 1. Introdução executiva..... | 5 |
| 2. Estratégico | 5 |
| 2.1 Introdução sobre a vulnerabilidade | 5 |
| 2.2 Sistemas, Segmentos e Produtos Afetados | 5 |
| 3. Estratégico | 7 |
| 3.1 Visão geral do NEXT.JSVisão geral do NEXT.JS | 7 |
| 3.2 Condições para exploração da vulnerabilidade | 7 |
| 4. Operacional | 9 |
| 4.1 Emulação da VulnerabilidadeEmulação da Vulnerabilidade..... | 9 |
| 4.2 Possibilidades de detecção | 10 |
| 4.3 Mitigação..... | 11 |
| 5. Conclusão | 12 |
| Referências | 13 |
| Autor | 13 |

LISTA DE TABELAS

| | |
|---|---|
| Tabela 1 - Condição de Exploração | 7 |
|---|---|

LISTA DE FIGURAS

| | |
|---|----|
| Figura 1 - Explorando o redirecionamento do middleware | 8 |
| Figura 2 - Requisição Legítima | 9 |
| Figura 3 - Requisição Maliciosa | 10 |
| Figura 4 - tráfego de rede com indícios de bypass por cabeçalho forjado | 11 |

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

2.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

O avanço no uso de frameworks modernos para aplicações *web*, como o **Next.js**, trouxe ganhos significativos em performance e escalabilidade, mas também introduziu novas superfícies de ataque. Um exemplo crítico é a vulnerabilidade [CVE-2025-29927](#), que afeta diretamente o mecanismo de **middlewares em cascata** utilizado por aplicações **baseadas em Next.js**.

Essa falha permite a **manipulação maliciosa do cabeçalho `x-middleware-subrequest`**, utilizado internamente pelo *framework*, possibilitando o *bypass* de autenticação e o acesso indevido a rotas protegidas. A exploração da **CVE-2025-29927** é simples, requer apenas requisições HTTP manipuladas, o que a torna especialmente perigosa em ambientes expostos à *internet*.

A vulnerabilidade representa risco elevado à confidencialidade e integridade de aplicações modernas, sendo categorizada como uma falha de **acesso inicial (Initial Access)** alinhada à técnica [T1190 – Exploit Public-Facing Application](#) do MITRE ATT&CK.

2.2 SISTEMAS, SEGMENTOS E PRODUTOS AFETADOS

A **CVE-2025-29927** afeta diretamente aplicações desenvolvidas com o *framework* **Next.js**, mantido pela **Vercel**. O impacto se dá especialmente em cenários que fazem uso extensivo do **Edge Middleware** para controle de autenticação e autorização.

Versões afetadas:

- **15.x até 15.2.2**
- **14.x até 14.2.24**
- **13.x até 13.5.8**
- **11.1.4 até 12.3.4**

Condições de risco adicional:

- Aplicações expostas diretamente à *internet*;
- Ambientes sem filtragem de cabeçalhos por *proxy* reverso;
- *Middleware* utilizado como única camada de validação;
- Ausência de checagem adicional nos *handlers* de rota.

Segmentos potencialmente impactados:

- **SaaS e plataformas digitais:** serviços que utilizam Next.js como backend de dashboards, áreas administrativas ou painéis de controle podem ser invadidos por atacantes não autenticados.
- **Setor financeiro e bancário:** aplicações que implementam autenticação via *middleware* em *endpoints* sensíveis podem sofrer acessos indevidos a dados financeiros.
- **Educação e e-learning:** plataformas de ensino que usam **Next.js** para controlar acesso a conteúdo ou gestão de alunos podem ter informações expostas ou alteradas.
- **Comércio eletrônico:** sistemas de gerenciamento de pedidos, estoques ou áreas restritas a lojistas ficam vulneráveis quando protegidos exclusivamente por middlewares.
- **Empresas que utilizam CDNs e Edge Functions:** ambientes com arquitetura distribuída em *edge computing* estão mais expostos a essa falha, especialmente sem proteção adicional em camadas intermediárias.

Organizações que utilizam **Next.js** em ambientes de produção devem **tratar essa vulnerabilidade com prioridade crítica, atualizando para versões corrigidas** e adotando medidas complementares de proteção, como **validação de cabeçalhos e checagens de autenticação** dentro das próprias rotas.

3. ESTRATÉGICO

3.1 VISÃO GERAL DO NEXT.JS

O **Next.js** é um *framework open source* de alto desempenho mantido pela *Vercel*, amplamente utilizado para o desenvolvimento de aplicações *web* modernas. Ele oferece suporte nativo a estratégias de renderização como **Server-Side Rendering (SSR)**, **Static Site Generation (SSG)** e **Client-Side Rendering**, sendo adotado por organizações que buscam escalabilidade, integração com **CDNs** e renderização otimizada para dispositivos móveis.

Entre suas funcionalidades mais importantes está o **Edge Middleware**, um mecanismo de interceptação de requisições **HTTP** executado antes da chegada à rota de destino. Esse *middleware* é comumente utilizado para autenticação, redirecionamentos e aplicação de políticas de segurança no perímetro da aplicação.

Contudo, esse recurso também introduz **dependência lógica crítica**, **especialmente quando utilizado como única camada de validação** para o acesso a rotas sensíveis.

3.2 CONDIÇÕES PARA EXPLORAÇÃO DA VULNERABILIDADE

A seguir, são apresentadas as principais condições que tornam uma aplicação Next.js vulnerável à exploração da **CVE-2025-29927**:

| Condição | Descrição |
|---|---|
| Validação de acesso exclusiva via <i>middleware</i> | Aplicações que utilizam apenas <i>middlewares</i> no <i>Edge Runtime</i> para controlar autenticação e autorização, sem validações adicionais nas rotas. |
| Aceitação do cabeçalho <i>x-middleware-subrequest</i> sem validação | O cabeçalho é processado mesmo quando enviado por clientes externos, permitindo que requisições maliciosas burlem os <i>middlewares</i> . |
| Ausência de <i>proxy</i> reverso ou <i>WAF</i> filtrando cabeçalhos | Ambientes sem filtragem intermediária permitem que o cabeçalho chegue diretamente à aplicação. |
| Rotas protegidas expostas diretamente | <i>Endpoints</i> sensíveis (como <i>/admin</i> , <i>/dashboard</i> , <i>/api/private</i>) acessíveis via GET/POST sem outras camadas de proteção. |
| Aplicações em <i>edge/CDN</i> sem regras de sanitização de <i>headers</i> | Arquiteturas <i>serverless</i> ou <i>edge</i> que propagam cabeçalhos sem higienização reforçam o risco de exploração. |

Tabela 1 - Condição de Exploração

O processo descrito acima é ilustrado na imagem a seguir, demonstrando como o cabeçalho malicioso permite contornar o middleware e acessar diretamente a rota protegida.

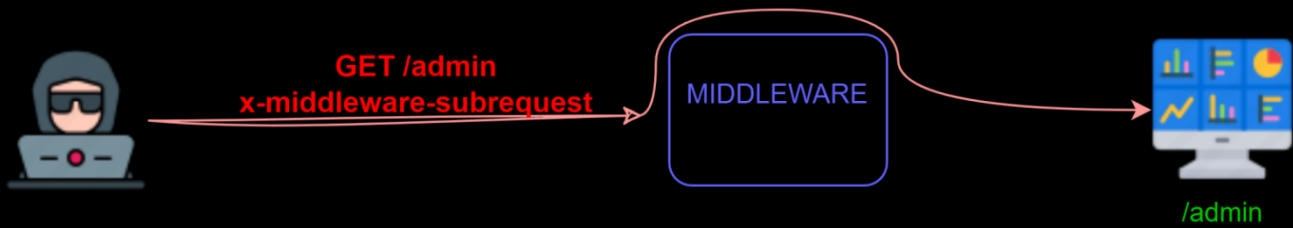


Figura 1 - Explorando o redirecionamento do middleware

4. OPERACIONAL

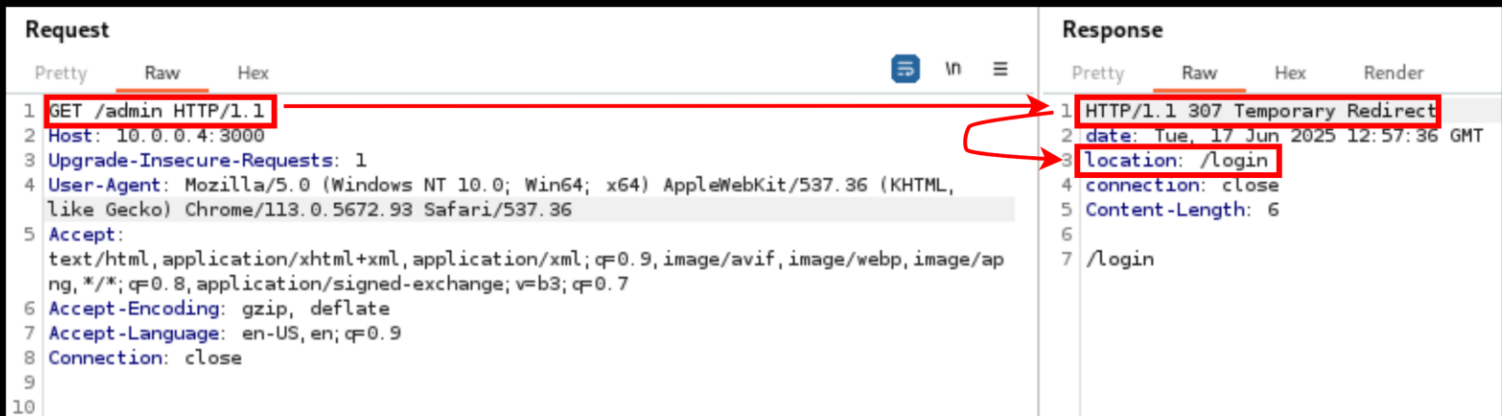
4.1 EMULAÇÃO DA VULNERABILIDADE

A exploração da **CVE-2025-29927** pode ser simulada em laboratório por meio de requisições **HTTP** manipuladas, demonstrando claramente o comportamento de **bypass** quando o cabeçalho **x-middleware-subrequest** é inserido manualmente.

Abaixo apresentamos dois cenários:

Requisição legítima com redirecionamento

Na imagem abaixo, vemos uma requisição legítima para a rota **/admin**, onde o **Next.js**, por meio do **middleware** de autenticação, retorna um redirecionamento **HTTP 307 Temporary Redirect** para a rota de **login (/login)**, conforme esperado.

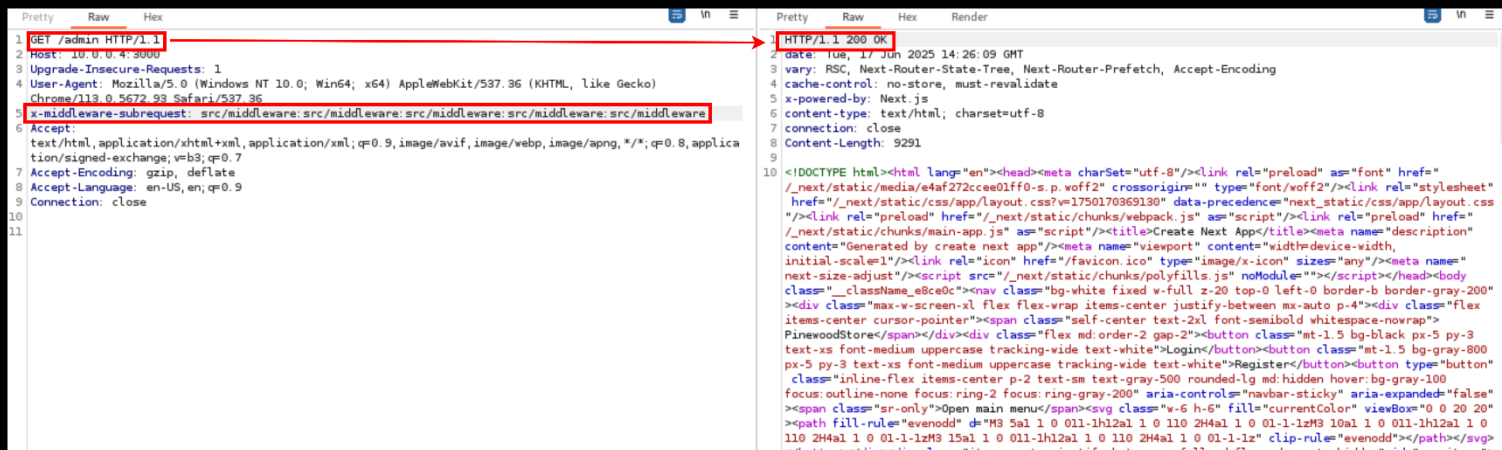


| Request | | | Response | | | |
|---------|---|-----|----------|-------------------------------------|-----|--------|
| Pretty | Raw | Hex | Pretty | Raw | Hex | Render |
| 1 | GET /admin HTTP/1.1 | | 1 | HTTP/1.1 307 Temporary Redirect | | |
| 2 | Host: 10.0.0.4:3000 | | 2 | date: Tue, 17 Jun 2025 12:57:36 GMT | | |
| 3 | Upgrade-Insecure-Requests: 1 | | 3 | location: /login | | |
| 4 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36 | | 4 | connection: close | | |
| 5 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 | | 5 | Content-Length: 6 | | |
| 6 | Accept-Encoding: gzip, deflate | | 6 | | | |
| 7 | Accept-Language: en-US,en;q=0.9 | | 7 | /login | | |
| 8 | Connection: close | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |

Figura 2 - Requisição Legítima

Requisição maliciosa com cabeçalho de subrequest

Na sequência, a mesma requisição é enviada com o cabeçalho *x-middleware-subrequest*. Isso faz com que o **Next.js** interprete erroneamente que a requisição já passou pela camada de *middleware*, permitindo o acesso direto à rota */admin*, sem exigir autenticação.



The screenshot displays two panels of network traffic analysis. The left panel shows the request details for a GET /admin HTTP/1.1 request. The 'x-middleware-subrequest' header is highlighted with a red box and a red arrow pointing to the right panel. The right panel shows the response details for an HTTP/1.1 200 OK response, with the status code and response type also highlighted with a red box. The response body contains HTML content for a Next.js application.

Figura 3 - Requisição Maliciosa

4.2 POSSIBILIDADES DE DETECÇÃO

A exploração da **CVE-2025-29927** pode ser identificada por meio da análise de tráfego de rede, especialmente em ambientes que contam com monitoramento em camadas como *proxies reversos*, *firewalls de aplicação (WAF)* ou ferramentas de *inspeção profunda de pacotes (DPI)*.

Uma das formas mais eficazes de detecção consiste na observação de requisições **HTTP** externas contendo o cabeçalho *x-middleware-subrequest*, direcionadas a rotas sensíveis da aplicação.

Além disso, a correlação entre essas requisições e respostas do tipo **HTTP<v> 200 OK** pode indicar que o acesso foi concedido indevidamente.

Abaixo, ilustramos esse cenário:

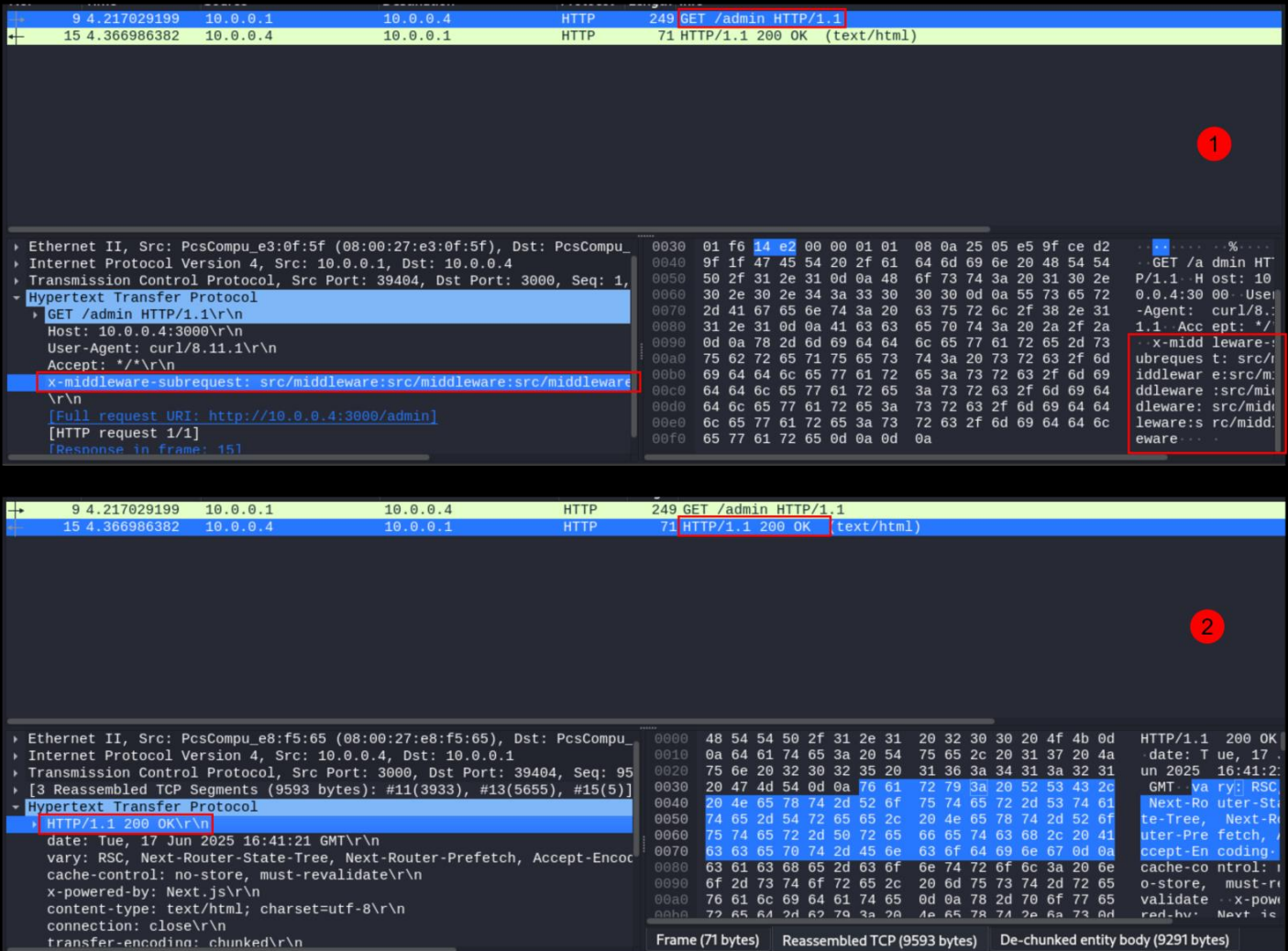


Figura 4 - tráfego de rede com indícios de bypass por cabeçalho forjado

4.3 MITIGAÇÃO

Para mitigar a [CVE-2025-29927](#), recomenda-se a adoção das seguintes ações:

1. Correção imediata

Atualizar o **Next.js** para versões corrigidas:

- 15.2.3+
- 14.2.25+
- 13.5.9+ ou 13.5.10+
- 12.3.5+

2. Mitigação temporária

Caso não seja possível aplicar o *patch* de forma imediata:

- Remover o cabeçalho **x-middleware-subrequest** em *proxies* ou WAFs;
- Bloquear requisições externas contendo esse cabeçalho via regras personalizadas.

3. Ações defensivas adicionais

- Implementar validação de autenticação diretamente nas rotas, além dos *middlewares*;
- Rejeitar qualquer cabeçalho **x-middleware-subrequest** vindo de fontes externas;
- Documentar e revisar toda a lógica de autenticação de rotas sensíveis.

5. CONCLUSÃO

A **CVE-2025-29927** evidência como a manipulação de cabeçalhos internos pode comprometer diretamente a lógica de segurança em aplicações desenvolvidas com o **Next.js**. A aplicação imediata das atualizações disponibilizadas pelos mantenedores do *framework* é a principal medida de contenção.

Essa vulnerabilidade reforça a importância de implementar **validações em múltiplas camadas**, evitando a dependência exclusiva de *middlewares*. Além disso, destaca-se a necessidade de adotar boas práticas como segmentação de acessos, monitoramento contínuo e estratégias de defesa em profundidade para garantir a resiliência de aplicações *web* modernas frente a vetores de ataque cada vez mais sofisticados.

REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- CTI Purple Team *by* ISH Tecnologia
- [MITRE ATT&CK](#)
- [POC](#)
- [NIST](#)

AUTOR

- Gustavo Jatene de Oliveira – Threat Researcher



heimdall
security research

A DIVISION OF ISH