TLP: CLEAR

BOLETIM DE SEGURANÇA

CVE-2024-55591 - Bypass de autenticação no WebSockets do Node.js

heimdall
security research

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

Uma falha de segurança classificada como bypass de autenticação por caminho ou canal alternativo [CWE-288] foi detectada nos sistemas FortiOS e FortiProxy. Rastreada como **CVE-2024-55591**, essa vulnerabilidade pode ser explorada por invasores remotos para obter privilégios de root.

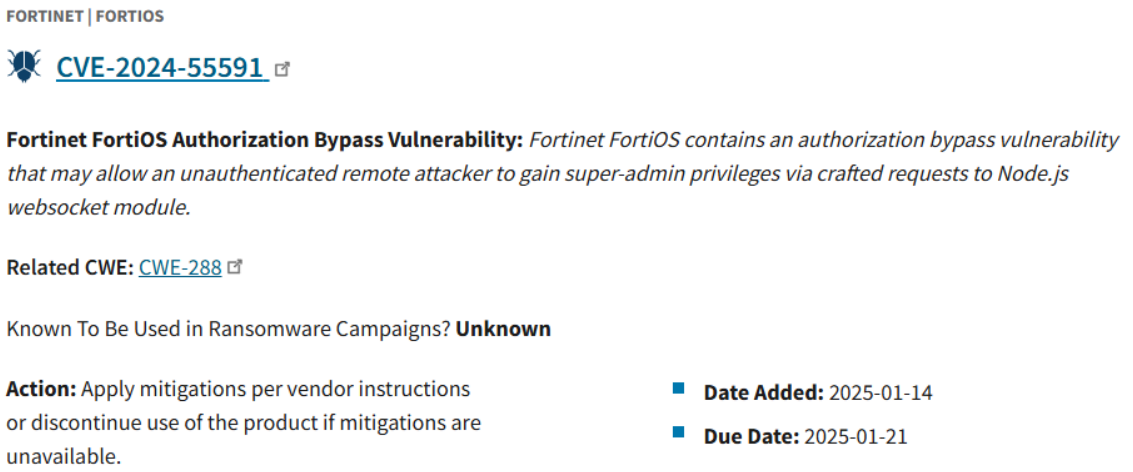
1.1 IMPACTO DA VULNERABILIDADE

Conforme avaliado, a exploração dessa vulnerabilidade pode resultar em:

- *Comprometimento total do sistema.*
- *Exfiltração de dados sensíveis.*
- *Interrupção de serviços.*
- *Propagação de ataques internos.*
- *Impacto reputacional e financeiro*

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-55591 categorizada como crítica, é uma falha que permite o invasor não autenticado obtenha privilégios de administrador de forma remota ao enviar solicitações especialmente criadas para o módulo websocket do Node.js. A exploração bem-sucedida dessa falha pode comprometer seriamente a segurança dos dispositivos afetados, permitindo controle total por parte do atacante, conforme a Fotiguard, há relatos de que a falha está sendo explorado ativamente em ataques.


FORTINET | FORTIOS

CVE-2024-55591

Fortinet FortiOS Authorization Bypass Vulnerability: *Fortinet FortiOS contains an authorization bypass vulnerability that may allow an unauthenticated remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module.*

Related CWE: CWE-288

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

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-01-14
- **Due Date:** 2025-01-21

Figura 1 – Vulnerabilidade no catalogo KEV-CISA.

Agência de Segurança de Infraestrutura e Cibersegurança dos EUA (CISA), anunciou a adição desta vulnerabilidade ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (**KEV**). Essa adição é baseada em evidências de explorações ativas, pois esse tipo de vulnerabilidade são vetores de ataque frequentes para atores mal-intencionados e representa riscos significativos para as organizações.

2.1 SISTEMAS E PRODUTOS AFETADOS

Abaixo segue os produtos e versões afetadas pela falha:

VERSÃO	PRODUTOS AFETADOS	CORREÇÃO
FortiOS 7.6	Não afetado	Não aplicável
FortiOS 7.4	Não afetado	Não aplicável
FortiOS 7.2	Não afetado	Não aplicável
FortiOS 7.0	7.0.0 a 7.0.16	Atualize para 7.0.17 ou superior
FortiOS 6.4	Não afetado	Não aplicável
FortiProxy 7.6	Não afetado	Não aplicável
FortiProxy 7.4	Não afetado	Não aplicável

FortiProxy 7.2	7.2.0 a 7.2.12	Atualize para 7.2.13 ou superior
FortiProxy 7.0	7.0.0 a 7.0.19	Atualize para 7.0.20 ou superior
FortiProxy 2.0	Não afetado	Não aplicável

Tabela 1 – Produtos afetados e suas correções.

3 RECOMENDAÇÕES

Atualização de software

- Instale imediatamente as versões corrigidas do FortiOS (7.0.17 ou superior) e do FortiProxy (7.0.20 ou 7.2.13 ou superiores) disponibilizadas pela Fortinet para corrigir essa falha.

Desativação de interfaces administrativas externas

- Desative o acesso HTTP/HTTPS às interfaces administrativas expostas na internet, reduzindo a superfície de ataque.

Restrição de IPs para acesso administrativo

- Configure políticas para permitir apenas endereços IP confiáveis a acessarem as interfaces administrativas dos dispositivos.

Habilitação de autenticação multifator (MFA)

- Implemente autenticação multifator (MFA) para acesso administrativo, adicionando uma camada extra de proteção mesmo em caso de credenciais comprometidas.

Monitoramento de constante

- Analise regularmente os logs do sistema para identificar atividades incomuns ou acessos não autorizados, principalmente no módulo websocket.

Segmentação de rede

- Isole os dispositivos Fortinet em segmentos de rede seguros, limitando sua comunicação com outros sistemas sensíveis ou críticos.

Treinamento e conscientização

- Capacite a equipe de TI para reconhecer vulnerabilidades e aplicar patches rapidamente. Além disso, mantenha uma política clara de resposta a incidentes para lidar com possíveis explorações.

4 INDICADORES DE COMPROMETIMENTO (IOC)

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de IPs e Domínios

Indicadores de IPs e Domínios	
IP	45.55[.]158[.]47 87.249[.]138[.]47 155.133[.]4[.]175 37.19[.]196[.]65 149.22[.]94[.]37

Tabela 2 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

4.1 OUTROS INDICADORES

Conforme a Fortiguard, foram observadas operações executadas pelo **Threat Actor**, nos casos que eles observaram incluíram parte ou todos os seguintes itens:

- *Criar uma conta de administrador no dispositivo com nome de usuário aleatório*
- *Criar uma conta de usuário local no dispositivo com nome de usuário aleatório*
- *Criar um grupo de usuários ou adicionar o usuário local acima a um grupo de usuários sslvpn existente*
- *Adicionar/alterar outras configurações (política de firewall, endereço de firewall, ...)*
- *Fazer login no sslvpn com os usuários locais adicionados acima para obter um túnel para a rede interna.*

O administrador ou usuário local criado pelo Threat Actor é gerado aleatoriamente. Como por exemplo:

- *Gujhmk*
- *Ed8x4k*
- *G0xgey*
- *Pvnw81*
- *Alg7c4*

- *Ypda8a*
- *Kmi8p4*
- *1a2n6t*
- *8ah1t6*
- *M4ix9f*
- *...etc...*

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Fortiguard**
- **NVD**

6 AUTORES

- **Leonardo Oliveira Silva**
- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH