BOLETIM DE SEGURANÇA

CISA adiciona falha crítica do Jenkins CVE-2024-23897 ao seu catálogo KEV

heimdall
security research
A DIVISION OF ISH

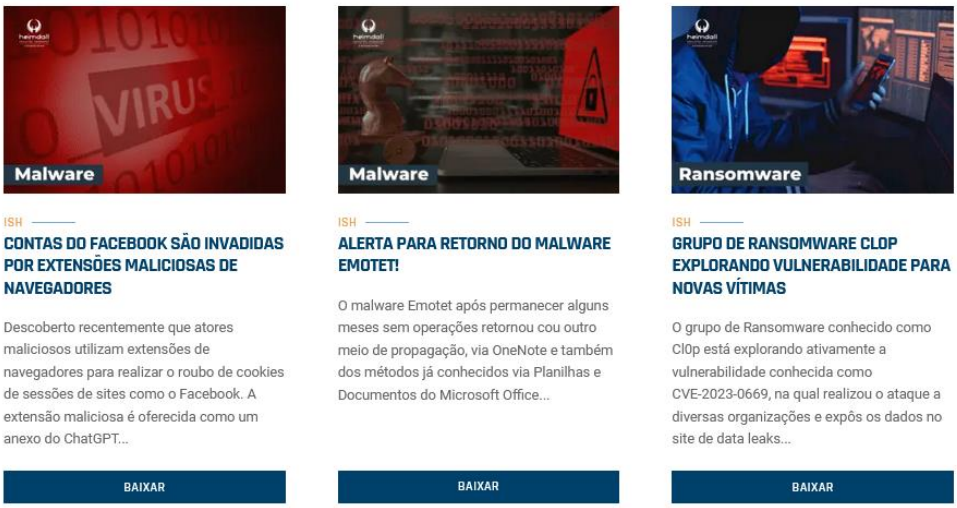
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[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 SUMÁRIO EXECUTIVO

Recentemente a Agência de Segurança de Infraestrutura e Cibersegurança dos EUA (CISA), anunciou a adição de **uma** nova 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 VULNERABILIDADE ADICIONADA AO KEV

A vulnerabilidade adicionada ao Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), é a seguinte:

CVE-2024-23897: Vulnerabilidade na interface de linha de comando (CLI) do **Jenkins**

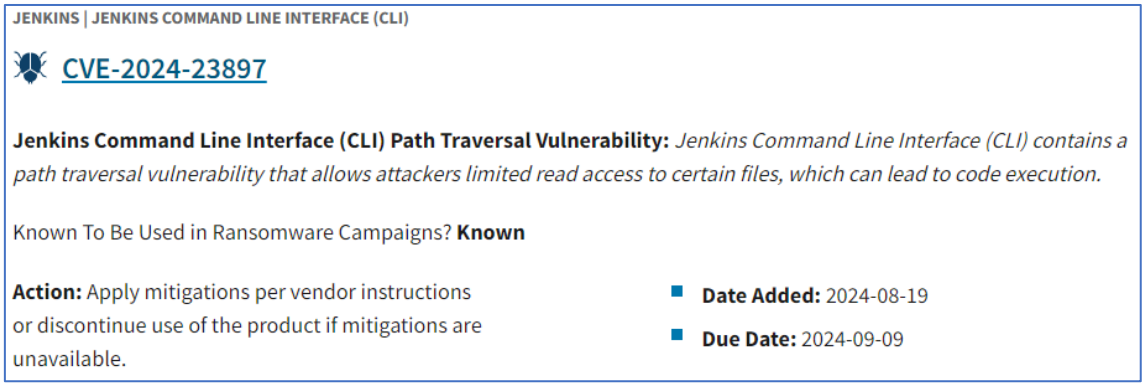


Figura 1 – Falha no catálogo da CISA-KEV.

Uma vulnerabilidade que afeta a interface de linha de comando (CLI) do Jenkins, ferramenta popular de integração contínua e automação. Essa vulnerabilidade permite que um atacante explore a funcionalidade da CLI do Jenkins para acessar arquivos e diretórios fora do diretório raiz permitido. Pois o Jenkins **2.441** e **versões anteriores**, **LTS 2.426.2** e versões **anteriores** não desabilita um recurso do seu analisador de comandos CLI que substitui um caractere '@' seguido por um caminho de arquivo em um argumento pelo conteúdo do arquivo.

Outros detalhes sobre a falha

- **Gravidade**: Crítica (CVSS Score: **9.8**)

Impacto

- **Confidencialidade:** Atacantes podem acessar arquivos confidenciais e dados sensíveis.
- **Integridade:** Potencial para modificação de arquivos críticos, levando a comprometimentos na integridade do sistema.
- **Disponibilidade:** Dependendo dos arquivos acessados e modificados, a disponibilidade do sistema pode ser impactada.

3 EXPLORAÇÕES OBSERVADAS DA VULNERABILIDADE

Como já mencionado, essa falha de segurança foi adicionada pela CISA, devido a explorações recentes por atores maliciosos, como o grupo **RansomEXX** e **Intelbroker**. Em um dos incidentes ocorridos, o ataque se originou de um servidor Jenkins mal configurado, desencadeando a cadeia de eventos. Em uma análise mais aprofundada, o agente da ameaça aproveitou o CVE-2024-23897 para obter acesso inicial não autorizado ao ambiente da vítima.

Em um outro incidente envolvendo o agente de ameaças Intelbroker, o ator identificou a falha CVE-2024-23897 em um servidor Jenkins exposto, usando essa vulnerabilidade, o agente de ameaça obtém acesso inicial ao servidor, explorando uma falha de inclusão de arquivos locais (LFI) para roubar chaves SSH. Com as chaves SSH comprometidas, o atacante acessa repositórios GitHub, como o do borngroup.com. Em seguida, o atacante realiza um despejo de todos os repositórios GitHub do grupo alvo. Por fim, o agente de ameaça utiliza chaves hardcoded e segredos encontrados no código-fonte roubado para infiltrar-se em outros sistemas e comprometer outras vítimas.

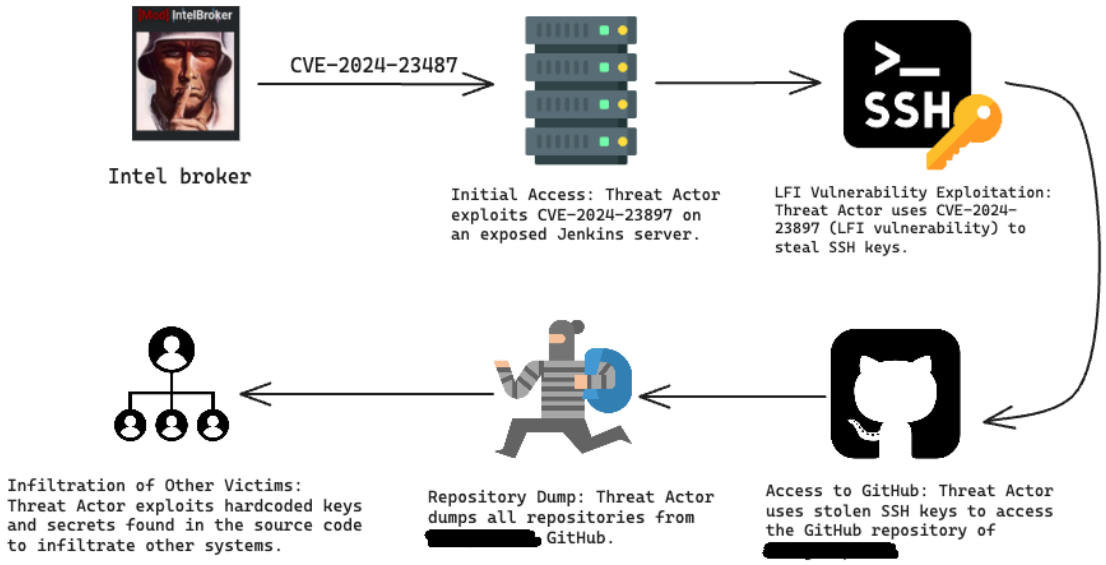


Figura 2 – Cadeia de ataque observada.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1190 Exploit Public-Facing Application	O ator da ameaça explorou a vulnerabilidade CVE-2024-23897 em um servidor Jenkins exposto para obter acesso inicial.
Credential Access	T1552.004 Unsecured Credentials: Private Keys	O ator da ameaça utilizou a vulnerabilidade CVE-2024-23897 para explorar uma vulnerabilidade LFI (Local File Inclusion), permitindo roubar chaves SSH armazenadas no sistema.
Lateral Movement	T1563.001 Remote Service Session Hijacking: SSH Hijacking	O uso de chaves privadas SSH extraídas para acessar outros sistemas dentro da rede.
Privilege Escalation	T1078 Valid Accounts	O ator da ameaça utilizou as chaves SSH roubadas para acessar o repositório GitHub.
Collection	T1560.001 Archive Collected Data: Archive via Utility T1602 Data from Configuration Repository	Coleta de dados sensíveis, como tokens de acesso e chaves privadas, de repositórios de configuração ou arquivos de configuração.
Impact	T1485 Data Destruction	Com o controle total, o atacante pode pode destruir dados críticos armazenados em sistemas acessados.

Tabela 1 – Tabela MITRE ATT&CK.

5 RECOMENDAÇÕES

Atualização do software

- Os administradores devem aplicar as atualizações mais recentes do Jenkins que corrigem essa vulnerabilidade.

Restrição de acesso

- Limitar o uso da CLI a ambientes seguros e usuários confiáveis.

Gerenciamento rigoroso de configuração

- As organizações devem implementar práticas rigorosas de gerenciamento de configuração para garantir que os sistemas sejam configurados com segurança e auditados regularmente.

Monitoramento continuo

- Implementar monitoramento rigoroso e auditoria de logs para identificar e responder rapidamente a tentativas de exploração.

Autenticação forte

- Imponha senhas fortes e implemente autenticação multifator (MFA) para todas as contas de usuário, especialmente aquelas com privilégios administrativos.

Auditorias de segurança regulares

- realize auditorias de segurança e testes de penetração regulares para identificar e abordar vulnerabilidades proativamente.

Inteligência de ameaças

- utilize inteligência de ameaças para entender os motivos, alvos e comportamentos de ataque de um agente de ameaça.

Esta vulnerabilidade destaca a necessidade crítica de manter ferramentas de automação como o Jenkins atualizadas e de aplicar boas práticas de segurança para limitar os vetores de ataque.

6 INDICADORES DE COMPROMISSOS

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 Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	fcd21c6fca3b9378961aa1865bee7ecb
sha1:	0abaa05da2a05977e0baf68838cff1712f1789e0
sha256:	4cae449450c07b7aa74314173c7b00d409eabfe22b86859f3b3acedd66010458
File name:	RansomEXXRANSOM.bin

Indicadores de compromisso do artefato	
md5:	9eacd598e62999467d4e3aadca6c4bc4
sha1:	6a3db79c1e2d44a7ee2eb66ff18a24b5e382be83
sha256:	ad635630ac208406cd28899313bef5d4e57dba163018dfb8924de90288e8bab3
File name:	Field Effect City

Indicadores de compromisso do artefato	
md5:	dc7cb3bfdc236c41f1c4bbac911daaa2
sha1:	8a3ca9efa2631435016a4f38ff153e52c647146e
sha256:	600be5ab7f0513833336bec705ca9bcfd1150a2931e61a4752b8de4c0af7b03a
File name:	webhook.php

Indicadores de compromisso do artefato	
md5:	092c44e78fcadb5e28bf4227d8f108bb
sha1:	285e0573ef667c6fb7aeb1608ba1af9e2c86b452
sha256:	b7f6edb98652e3de989c0b8a54b7a8b02053c32883114cd28dd035350a9896d3
File name:	tinkoff.php

Indicadores de compromisso do artefato	
md5:	fce9de7cfeadf6aab90734ca9bc0eab2
sha1:	26727d5fceef79de2401ca0c9b2974cd99226dcb
sha256:	4f1a6058f7cd89ab378de10b4b27ca964c9671fb3724a8c5519606626520e5ef
File name:	scam.php

Indicadores de compromisso do artefato	
md5:	dc7cb3bfdc236c41f1c4bbac911daaa2
sha1:	8a3ca9efa2631435016a4f38ff153e52c647146e
sha256:	600be5ab7f0513833336bec705ca9bcfd1150a2931e61a4752b8de4c0af7b03a
File name:	webhook.php

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URLs	
URL	olx[.]id7423[.]ru boxberry[.]id7423[.]ru avito-rent[.]id7423[.]ru 3inf[.]site

Tabela 3 – Indicadores de Compromissos 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.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- CISA
- NVD
- MITRE ATT&CK
- Jenkins
- Juniper
- Cloudsek

8 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH