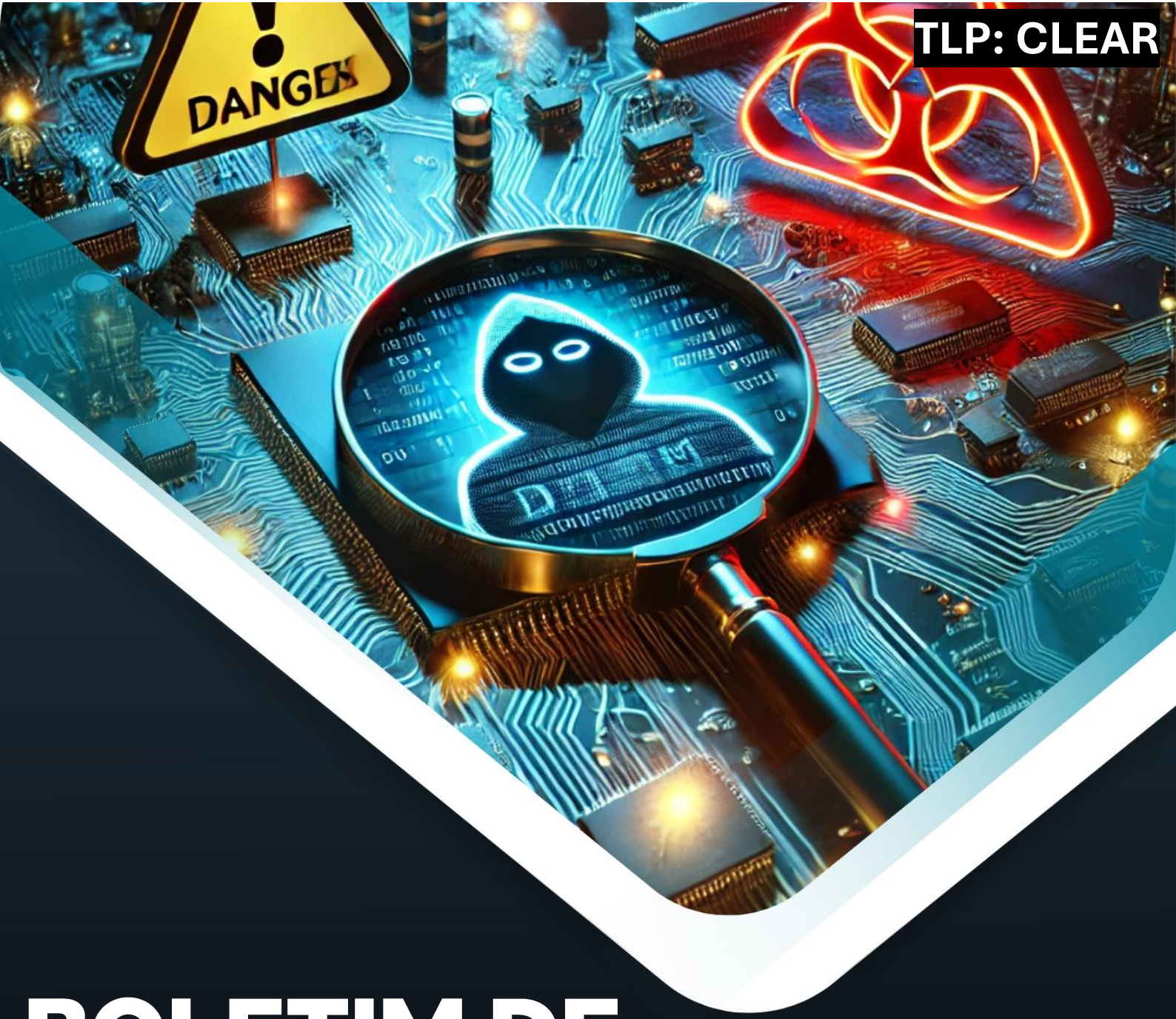
TLP: CLEAR



BOLETIM DE SEGURANÇA

Ivanti alerta sobre vulnerabilidade de zero day explorada no Connect Secure

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 FIGURAS

1 INTRODUÇÃO EXECUTIVA

A **Ivanti** informou que criminosos cibernéticos estão explorando uma vulnerabilidade de execução remota de código identificada como **CVE-2025-0282** em ataques de zero day para comprometer dispositivos e instalar malware. A descoberta ocorreu após a identificação de atividades suspeitas nos sistemas de clientes. Nesta investigação, a empresa confirmou que a falha estava sendo explorada ativamente por agentes maliciosos.

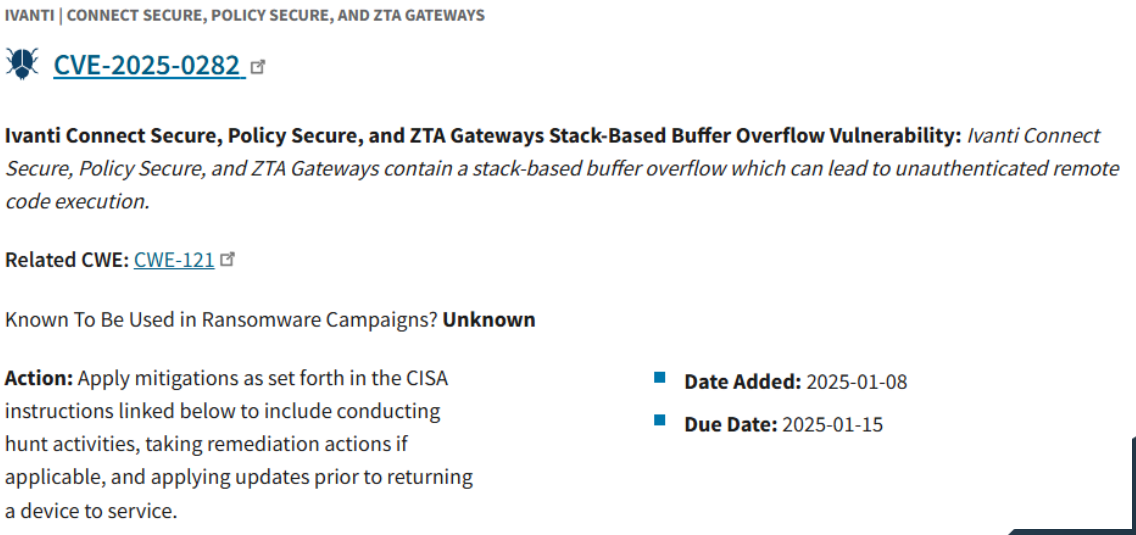
2 INFORMAÇÃO SOBRE A VULNERABILIDADE

A falha CVE-2025-0282 é classificada como crítica e envolve um estouro de buffer baseado em pilha, afetando as versões anteriores à *22.7R2.5* do **Ivanti Connect Secure**, à *22.7R1.2* do **Ivanti Policy Secure** e à *22.7R2.3* do **Ivanti Neurons para ZTA gateways**. A brecha permite que invasores não autenticados executem código remotamente nos dispositivos comprometidos. Apesar de a vulnerabilidade impactar esses três produtos, a Ivanti relatou que apenas dispositivos Connect Secure foram alvo de ataques até o momento. "Identificamos um número limitado de dispositivos Connect Secure explorados pelo CVE-2025-0282. Não há indícios de que as vulnerabilidades estejam sendo usadas contra o Ivanti Policy Secure ou Neurons para ZTA gateways", explicou a empresa em um comunicado oficial.

Como resposta, a Ivanti lançou atualizações de segurança para corrigir a vulnerabilidade no Connect Secure, com a versão de firmware *22.7R2.5* resolvendo o problema. A empresa reforça que a solução não deve ser exposta diretamente à Internet, o que reduz significativamente o risco de exploração. A correção para o Ivanti Policy Secure está programada para ser disponibilizada em 21 de janeiro de 2025, e será distribuída por meio do portal oficial de downloads da Ivanti. Enquanto isso, a empresa reforça a importância de manter os dispositivos IPS configurados conforme suas recomendações e protegidos contra exposição indevida à Internet.

2.1 VULNERABILIDADE ADICIONADA AO KEV-CISA

A CISA incluiu essa falha em seu catálogo de vulnerabilidades exploradas, conhecido como KEV-CISA, em razão das contínuas explorações realizadas por atores maliciosos. Essas explorações têm como objetivo infectar dispositivos com malwares personalizados, conforme também destacado em um relatório publicado pela Mandiant.


IVANTI | CONNECT SECURE, POLICY SECURE, AND ZTA GATEWAYS

CVE-2025-0282

Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability: *Ivanti Connect Secure, Policy Secure, and ZTA Gateways contain a stack-based buffer overflow which can lead to unauthenticated remote code execution.*

Related CWE: CWE-121

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

Action: Apply mitigations as set forth in the CISA instructions linked below to include conducting hunt activities, taking remediation actions if applicable, and applying updates prior to returning a device to service.

- **Date Added:** 2025-01-08
- **Due Date:** 2025-01-15

Figura 1 – Vulnerabilidade CVE-2025-0282 no catalogo KEV-CISA.

3 RECOMENDAÇÕES

Para mitigar os riscos associados a essa falha, a Ivanti recomenda as seguintes tomadas de ações:

Atualização imediata

- **Ivanti Connect Secure:** Atualize para a versão 22.7R2.5 ou superior, que já está disponível.
- Ivanti Policy Secure e Neurons para gateways ZTA: Aguarde o lançamento dos patches previstos para 21 de janeiro de 2025 e, assim que disponíveis, realize a atualização.

Verificação de integridade

- Utilize a ferramenta de verificação de integridade (ICT) fornecida pela Ivanti para identificar possíveis comprometimentos. Certifique-se de que a ferramenta esteja atualizada e compatível com a versão do seu dispositivo.

Ações baseadas nos resultados da ICT

Sem sinais de comprometimento:

- Realize uma redefinição de fábrica no dispositivo antes de aplicar a atualização para garantir um ambiente limpo.

Com sinais de comprometimento:

- Efetue uma redefinição de fábrica para remover qualquer malware presente antes de recolocar o dispositivo em produção.

Configuração de segurança

- Assegure-se de que os dispositivos estejam configurados conforme as recomendações de segurança da Ivanti, evitando exposições desnecessárias à internet.

Monitoramento contínuo

- Mantenha uma vigilância constante sobre os dispositivos e a rede, utilizando ferramentas de monitoramento para detectar atividades suspeitas ou anômalas.

Revisão de credenciais

- Considere redefinir senhas e chaves de acesso associadas aos dispositivos afetados, especialmente se houver indícios de comprometimento.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Ivanti**
- **CVE**
- **Cloud.google**
- **Bleeping Computer**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH