BOLETIM DE SEGURANÇA

Nova falha RCE do Ivanti afetando milhares de gateways VPN expostos.

heimdall
security research
A DIVISION OF ISH

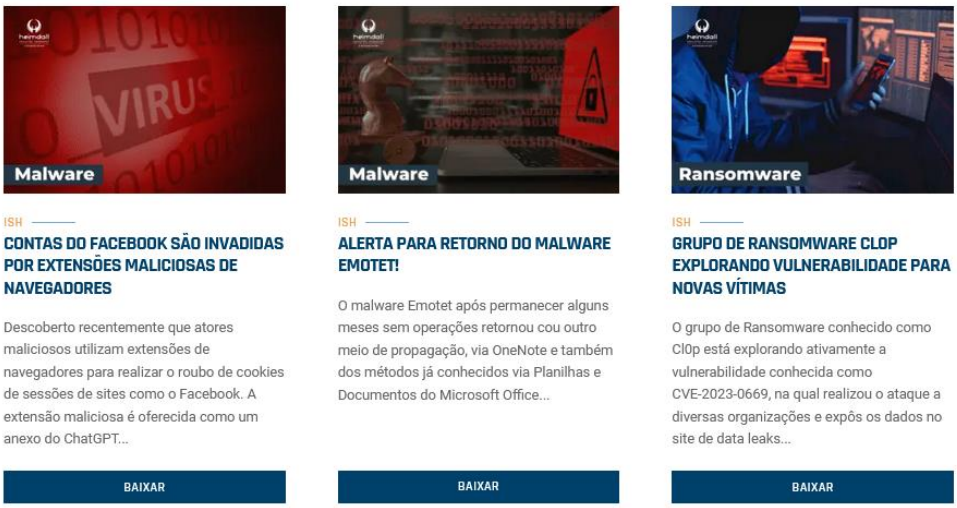
TLP: CLEAR

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 FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente a Ivanti publicou sobre a vulnerabilidade CVE-2024-21894 classificada como crítica que foi descoberta nos gateways *Ivanti Connect Secure* (**ICS**), (anteriormente conhecido como Pulse Connect Secure) e *Ivanti Policy Secure*.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A Shadowserver relatou que cerca de 16.500 instâncias são vulneráveis à falha RCE, expostos na Internet.

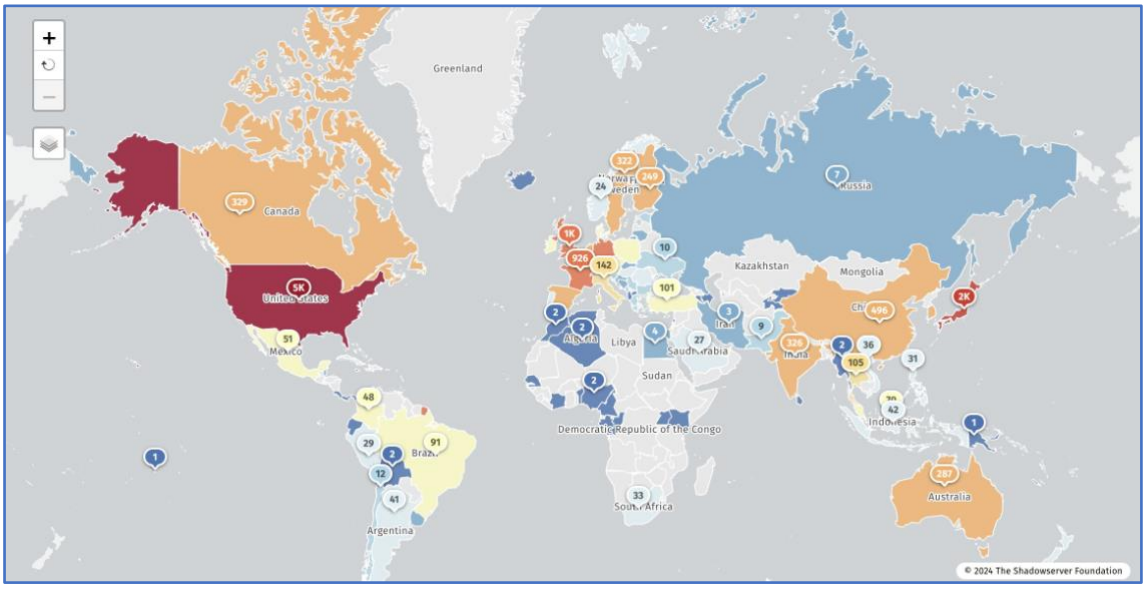


Figura 1 – Endpoints vulneráveis da Ivanti em todo o mundo.

Nos Estados Unidos, registra-se o maior número de casos, totalizando 4.700. Seguem na lista o Japão com 2.000 casos, o Reino Unido com 1.000, e Alemanha e França com 900 cada. Menores incidências são observadas na China, Holanda e Espanha, com 500 casos cada, além de Canadá e Índia com 330, e Suécia com 320. Esses dados refletem um padrão global de vulnerabilidades críticas nos produtos Ivanti, que frequentemente se tornam brechas para ataques em organizações internacionais. No Brasil esses dispositivos expostos, possuem um número pequeno, porém merecem uma devida atenção.

A vulnerabilidade CVE-2024-21894 é uma falha de heap overflow no componente IPSec do Ivanti Connect Secure (9.x, 22.x) e Ivanti Policy Secure permitindo que um usuário mal-intencionado não autenticado envie solicitações especialmente criadas para travar o serviço, causando assim um ataque DoS. Em certas condições, isso pode levar à execução de código arbitrário.

Um estudo realizado pela Mandiant detalhou ataques recentes a endpoints Ivanti, destacando a atuação de hackers chineses organizados em cinco grupos distintos e o uso do malware 'SPAWN'. Administradores de sistemas são instados a aplicar correções e mitigações, especialmente para a CVE-2024-21894, conforme orientações do fabricante.

3 RECOMENDAÇÕES

A Ivanti informou que já encontra-se disponível um patch para todas as versões suportadas do produto por meio do portal de download, recomendando que os clientes realizem a atualização imediatamente para garantir que estejam protegidos. Abaixo mostra as versões de patch disponíveis:

Patch versions:

- *Ivanti Connect Secure:* 22.1R6.2, 22.2R4.2, 22.3R1.2, 22.4R1.2, 22.4R2.4, 22.5R1.3, 22.5R2.4, 22.6R2.3, 9.1R14.6, 9.1R15.4, 9.1R16.4, 9.1R17.4 e 9.1R18.5.
- *Ivanti Policy Secure:* 22.4R1.2, 22.5R1.3, 22.6R1.2, 9.1R16.4, 9.1R17.4 e 9.1R18.5.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Ivanti**
- **Post ShadowsServers**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH