
# BOLETIM DE SEGURANÇA

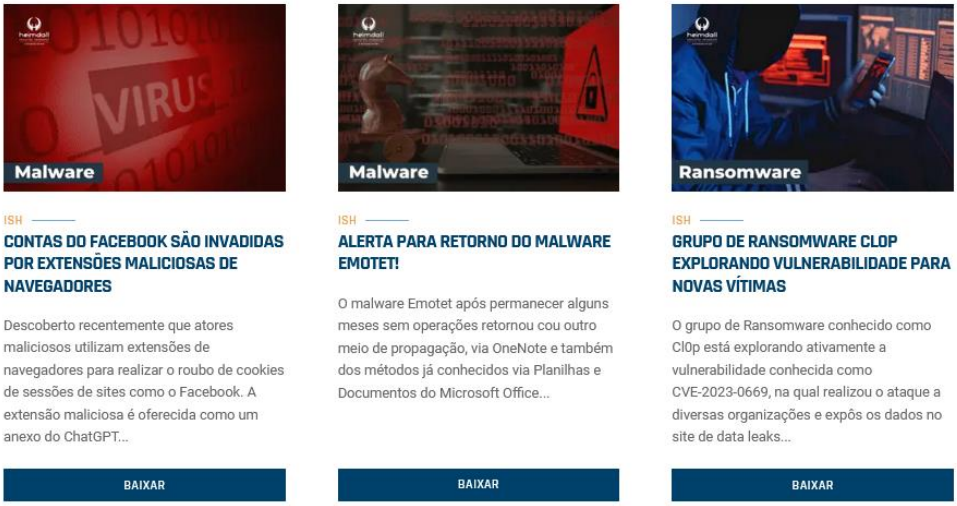
## Ivanti alerta para nova vulnerabilidade crítica no Ivanti Cloud Appliance sendo explorada

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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

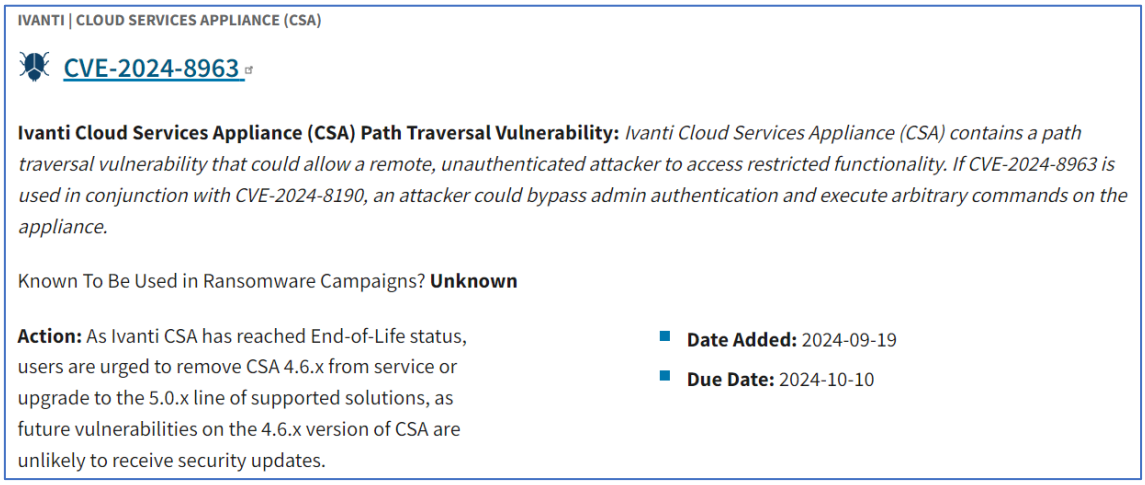
A Ivanti anunciou a descoberta de uma vulnerabilidade CVE-2024-8963 categorizada como crítica que afeta o Cloud Service Appliance (CSA). A falha de segurança, está sendo ativamente explorada por cibercriminosos, colocando em risco a integridade de sistemas que ainda não aplicaram as correções adequadas.

## 2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Uma nova vulnerabilidade, catalogada como CVE-2024-8963, recebeu uma pontuação **CVSS de 9,4** em 10, destacando sua gravidade. Essa falha permite que invasores remotos, sem autenticação, acessem funcionalidades restritas do ***Cloud Service Appliance*** (CSA), explorando o recurso de Path Traversal.

Em um comunicado oficial, a Ivanti esclareceu que o problema foi resolvido com a atualização do patch, mas a falha pode ser combinada com outra vulnerabilidade CVE-2024-8190, que possui um CVSS de 7,2. Juntas, essas falhas permitem que invasores contornem a autenticação de administrador e executem comandos arbitrários nos dispositivos.

Além disso, a empresa informou que, até o momento, já tem conhecimento de um número limitado de clientes que foram explorados por meio dessa vulnerabilidade. Dias antes, foram registradas tentativas de exploração ativa relacionadas ao CVE-2024-8190. Essas duas falhas, quando combinadas, podem ser utilizadas por agentes maliciosos para obter acesso e executar códigos maliciosos em dispositivos vulneráveis. Esse cenário levou a Agência de Segurança Cibernética e de Infraestrutura (CISA) a incluir a vulnerabilidade no catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), dizendo que tal vulnerabilidade é “um vetor de ataque frequente para atore cibernéticos maliciosos”.



IVANTI | CLOUD SERVICES APPLIANCE (CSA)

CVE-2024-8963

**Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability:** *Ivanti Cloud Services Appliance (CSA) contains a path traversal vulnerability that could allow a remote, unauthenticated attacker to access restricted functionality. If CVE-2024-8963 is used in conjunction with CVE-2024-8190, an attacker could bypass admin authentication and execute arbitrary commands on the appliance.*

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

**Action:** As Ivanti CSA has reached End-of-Life status, users are urged to remove CSA 4.6.x from service or upgrade to the 5.0.x line of supported solutions, as future vulnerabilities on the 4.6.x version of CSA are unlikely to receive security updates.

- **Date Added:** 2024-09-19
- **Due Date:** 2024-10-10

*Figura 1 – Vulnerabilidades no catálogo KEV-CISA.*

# 3 RECOMENDAÇÕES

A Ivanti emitiu patches de segurança para mitigar o problema e recomenda que todas as organizações afetadas implementem as correções o mais rápido possível para evitar ataques cibernéticos.

# 4 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- Ivanti
- Thehackernews
- NVD

# 5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH