TLP: CLEAR

BOLETIM DE SEGURANÇA

A Ivanti informa sobre três vulnerabilidades no CSA que exploradas ativamente

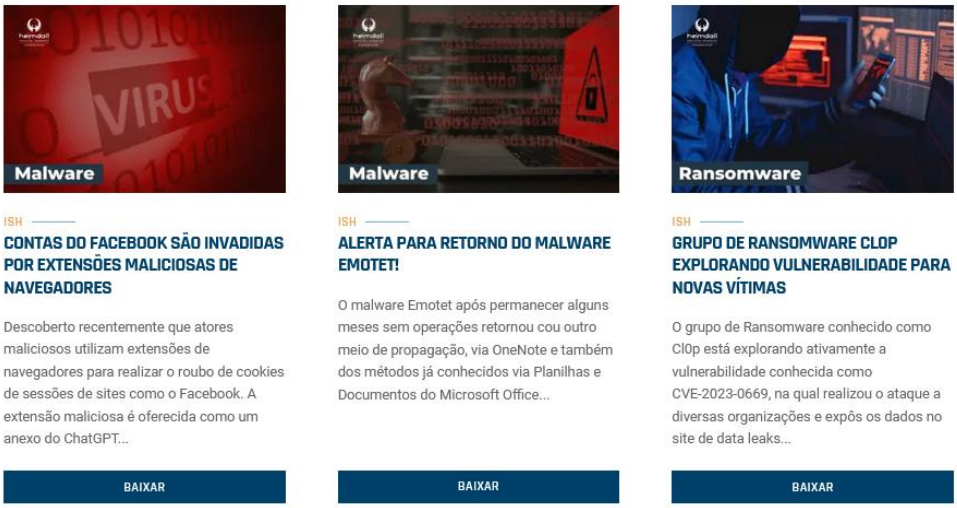
heimdall
security research
A DIVISION OF ISH

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 SUMÁRIO EXECUTIVO

A Ivanti emitiu um alerta sobre três novas vulnerabilidades de segurança em seu Cloud Service Appliance (CSA), que estão sendo ativamente exploradas. Essas falhas, se exploradas com sucesso, podem permitir que invasores autenticados com privilégios de administrador ignorem restrições, executem comandos SQL arbitrários ou obtenham execução remota de código.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

As recentes vulnerabilidades de *zero day* no Ivanti CSA estão sendo exploradas em conjunto com uma falha corrigida no mês passado, conforme relatado pela empresa de software sediada em Utah.

A exploração dessas falhas pode permitir que invasores autenticados com privilégios de administrador ignorem restrições, executem comandos SQL arbitrários ou obtenham execução remota de código.

A Ivanti informou que um número limitado de clientes que utilizam o CSA 4.6 patch 518 e versões anteriores foram afetados quando as vulnerabilidades **CVE-2024-9379, CVE-2024-9380** ou **CVE-2024-9381** foram combinadas com a **CVE-2024-8963**.

Não há evidências de exploração em ambientes que utilizam o CSA 5.0. As três vulnerabilidades são descritas abaixo:

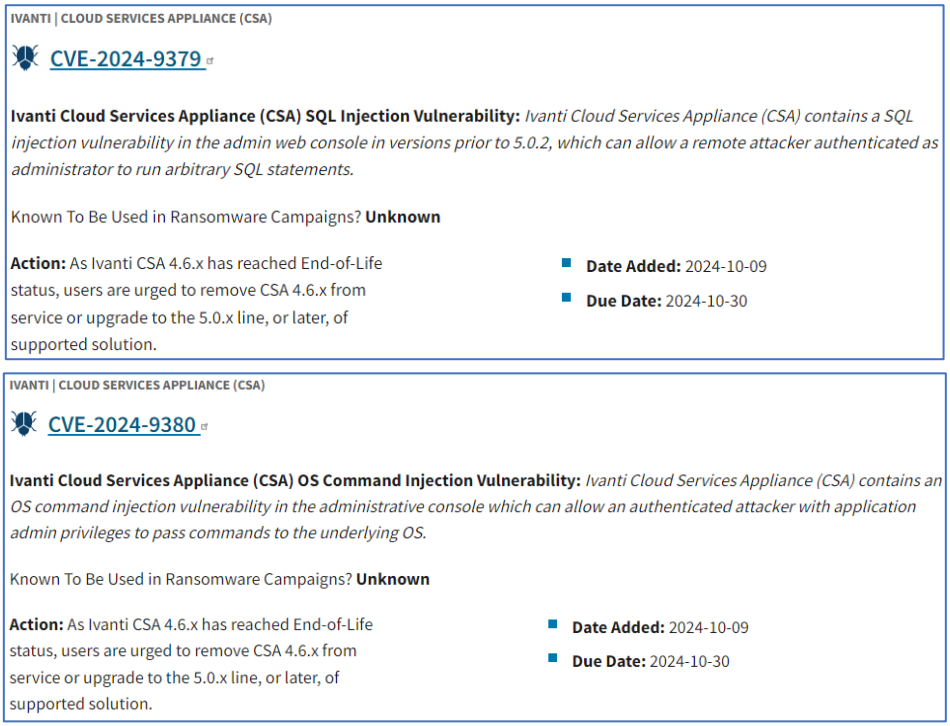
- CVE-2024-9379: Esta vulnerabilidade trata-se de um **SQL injection** no console da web do administrador do Ivanti CSA antes da versão 5.0.2, permitindo a execução de comandos SQL arbitrários por um invasor autenticado com privilégios de administrador.
- CVE-2024-9380: Essa vulnerabilidade trata-se está relacionada ao ataque de **Command injection** do sistema operacional no console da web do administrador do Ivanti CSA antes da versão 5.0.2, permitindo a execução remota de código por um invasor autenticado com privilégios de administrador.
- CVE-2024-9381: Esta vulnerabilidade trata-se de um **Path Traversal** no Ivanti CSA antes da versão 5.0.2, permitindo que um invasor autenticado com privilégios de administrador ignore restrições.

Os ataques observados combinam essas falhas com a CVE-2024-8963, uma vulnerabilidade crítica de travessia de caminho que permite acesso não autorizado a funcionalidades restritas. Ivanti descobriu essas novas falhas durante a investigação das explorações das vulnerabilidades CVE-2024-8963 e CVE-2024-8190, outra falha de injeção de comando do sistema operacional no CSA, que já foi corrigida.

Além de atualizar para a versão 5.0.2, a Ivanti recomenda que os usuários revisem seus dispositivos em busca de sinais de comprometimento, como usuários administrativos modificados ou adicionados recentemente, e verifiquem alertas de ferramentas de detecção e resposta de endpoint (EDR) instaladas. Este desenvolvimento ocorre menos de uma semana após a CISA adicionar uma falha de segurança no Ivanti Endpoint Manager (EPM), corrigida em maio (CVE-2024-29824), ao catálogo de Vulnerabilidades Exploradas Conhecidas (KEV).

3 VULNERABILIDADES NO CATÁLOGO KEV-CISA

A agência de segurança cibernética (CISA) adicionou as falhas ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), dizendo que tais vulnerabilidades são **"vetores de ataque frequentes para atores cibernéticos maliciosos".**



IVANTI | CLOUD SERVICES APPLIANCE (CSA)

CVE-2024-9379

Ivanti Cloud Services Appliance (CSA) SQL Injection Vulnerability: *Ivanti Cloud Services Appliance (CSA) contains a SQL injection vulnerability in the admin web console in versions prior to 5.0.2, which can allow a remote attacker authenticated as administrator to run arbitrary SQL statements.*

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

Action: As Ivanti CSA 4.6.x 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, or later, of supported solution.

- **Date Added:** 2024-10-09
- **Due Date:** 2024-10-30

IVANTI | CLOUD SERVICES APPLIANCE (CSA)

CVE-2024-9380

Ivanti Cloud Services Appliance (CSA) OS Command Injection Vulnerability: *Ivanti Cloud Services Appliance (CSA) contains an OS command injection vulnerability in the administrative console which can allow an authenticated attacker with application admin privileges to pass commands to the underlying OS.*

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

Action: As Ivanti CSA 4.6.x 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, or later, of supported solution.

- **Date Added:** 2024-10-09
- **Due Date:** 2024-10-30

Figura 1 – Vulnerabilidades no catálogo KEV-CISA.

4 RECOMENDAÇÕES

A empresa recomenda a atualização para a versão **mais recente (5.0.2)** e a revisão de dispositivos para sinais de comprometimento.

5 REFERÊNCIAS

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

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH