



# RELATÓRIO DE PESQUISAS

## Web & Mobile Threat Emulation

Quando a configuração compromete: Explorando a **CVE-2025-24813** no Apache Tomcat




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

 <p><b>Malware</b></p>	 <p><b>Malware</b></p>	 <p><b>Ransomware</b></p>
<p>ISH</p> <p><b>CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES</b></p> <p>Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...</p>	<p>ISH</p> <p><b>ALERTA PARA RETORNO DO MALWARE EMOTET!</b></p> <p>O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...</p>	<p>ISH</p> <p><b>GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS</b></p> <p>O grupo de Ransomware conhecido como Clop está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...</p>
<p>BAIXAR</p>	<p>BAIXAR</p>	<p>BAIXAR</p>

## SUMÁRIO

1	Introdução executiva .....	5
2	Estratégico.....	5
2.1	Introdução sobre a vulnerabilidade .....	5
2.2	Sistemas, segmentos e produtos afetados .....	5
3	Tático .....	8
3.1	Visão geral do Apache Tomcat .....	8
3.2	Condições para exploração da vulnerabilidade .....	8
3.3	Tabela MITRE ATT&CK.....	10
4	Conclusão .....	11
5	Recomendações.....	12
6	Referências .....	14
7	Autores.....	14

## LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK. ....	10
--------------------------------------	----

## LISTA DE FIGURAS

Figura 1 – CVE-2025-24813 adicionada ao catálogo KEV-CISA.....	6
Figura 2 – Diagrama exploração Tomcat CVE-2025-24813. ....	9

## 1 INTRODUÇÃO EXECUTIVA

---

Este relatório de segurança, desenvolvido pela equipe de inteligência **Heimdall da ISH Tecnologia**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: **Estratégico**, **Tático** e **Operacional**, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

## 2 ESTRATÉGICO

---

### 2.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

A crescente digitalização dos processos empresariais e a dependência de aplicações web para operações críticas tornam a cibersegurança uma prioridade estratégica nas organizações. Nesse contexto, a identificação e resposta ágil a vulnerabilidades emergentes são essenciais para a proteção de dados, continuidade dos negócios e resiliência operacional frente a ameaças cada vez mais sofisticadas.

Um exemplo relevante é a vulnerabilidade [CVE-2025-24813](#), recentemente identificada no **Apache Tomcat**, uma das plataformas de servidor web mais utilizadas globalmente. Essa falha pode representar riscos significativos à **confidencialidade**, **integridade** e **disponibilidade** das aplicações expostas, especialmente em ambientes que utilizam requisições HTTP com métodos de escrita habilitados.

### 2.2 SISTEMAS, SEGMENTOS E PRODUTOS AFETADOS

A vulnerabilidade CVE-2025-24813 afeta diretamente servidores que utilizam versões vulneráveis do Apache Tomcat, uma tecnologia amplamente empregada por organizações em diversos setores para hospedagem de aplicações Java baseadas em web.

#### **Sistemas e produtos afetados:**

- **Apache Tomcat** nas versões:
  - 9.0.0.M1 até 9.0.98
  - 10.1.0-M1 até 10.1.34
  - 11.0.0-M1 até 11.0.2
- Ambientes no qual é habilitada a **escrita no default servlet**.
- Sistemas que fazem uso de **requisições HTTP PUT parciais**.



- Infraestruturas que utilizam **persistência de sessão baseada em arquivos**.
- Aplicações com bibliotecas suscetíveis à **desserialização insegura**.

#### Segmentos potencialmente impactados:



- **Setor financeiro:** aplicações bancárias internas e de internet banking podem ser comprometidas, expondo dados sensíveis de clientes e permitindo movimentações não autorizadas, caso a vulnerabilidade seja explorada com sucesso.
- **Serviços de governo eletrônico (e-Gov):** portais de atendimento ao cidadão, sistemas de arrecadação e plataformas de serviços públicos correm risco de invasão e manipulação de dados, podendo afetar a confiabilidade e continuidade dos serviços oferecidos à população.
- **Saúde:** sistemas de gestão hospitalar e de prontuários eletrônicos podem ser alvos de ataques visando o sequestro ou vazamento de informações médicas sigilosas, impactando diretamente o atendimento e a privacidade dos pacientes.
- **Educação:** plataformas de ensino à distância e portais acadêmicos podem sofrer alterações indevidas, como inserção de conteúdos maliciosos, vazamento de dados de alunos e interrupção de serviços essenciais ao ensino remoto.
- **Tecnologia da Informação e Telecomunicações:** provedores de serviços e empresas de tecnologia que utilizam Tomcat como base de APIs REST ou aplicações web podem se tornar vetores para ataques em cadeia, comprometendo não apenas seus sistemas, mas também os de clientes integrados.

Organizações que operam infraestruturas expostas à internet, ambientes em nuvem ou que realizam operações críticas online devem considerar essa falha como prioridade máxima de mitigação, com ações imediatas de correção, revisão de configuração e monitoramento de segurança.

APACHE | TOMCAT

 [CVE-2025-24813](#) 

**Apache Tomcat Path Equivalence Vulnerability:** *Apache Tomcat contains a path equivalence vulnerability that allows a remote attacker to execute code, disclose information, or inject malicious content via a partial PUT request.*

Related CWEs: [CWE-44](#)  | [CWE-502](#) 

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

**Action:** Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

■ **Date Added:** 2025-04-01

■ **Due Date:** 2025-04-22

Figura 1 – CVE-2025-24813 adicionada ao catálogo KEV-CISA.

A inclusão da CVE-2025-24813 no catálogo *Known Exploited Vulnerabilities (KEV)* da **CISA** reforça que essa falha vai além de um problema técnico, trata-se de uma vulnerabilidade com **risco real e comprovado de exploração ativa**, especialmente em ambientes que utilizam o Apache Tomcat com configurações inadequadas. Sua presença nesse catálogo indica que a ameaça já foi observada em cenários reais e, portanto, requer atenção imediata. Diante disso, **as organizações devem tratá-la como uma prioridade crítica de segurança**, adotando medidas corretivas com urgência, revisando suas configurações e reforçando os controles de exposição em ambientes web.

## 3 TÁTICO

---

### 3.1 VISÃO GERAL DO APACHE TOMCAT

O **Apache Tomcat** é um dos servidores de aplicação Java mais utilizados no mundo, oferecendo suporte para as especificações **Servlet**, **JSP** e **WebSocket**. Ele atua como um contêiner de *servlets*, processando requisições **HTTP** e executando código *Java* dinâmico em ambientes corporativos e aplicações *web*.

Dentre seus componentes internos, destaca-se o *Default Servlet*, responsável por servir arquivos estáticos. Embora por padrão ele não permita escrita, esse comportamento pode ser ajustado por meio da configuração do *servlet* em arquivos como o **web.xml**, em casos específicos, habilitando a funcionalidade de *upload* de conteúdo. Quando essa permissão de escrita é combinada com *partial PUT*, abrem-se vetores perigosos para manipulação de arquivos.

Além disso, o *Tomcat* oferece um mecanismo de persistência de sessão baseada em arquivos, que pode ser abusado por atacantes em cenários de **RCE** caso bibliotecas vulneráveis à desserialização estejam presentes no *classpath*.

### 3.2 CONDIÇÕES PARA EXPLORAÇÃO DA VULNERABILIDADE

A exploração da vulnerabilidade **CVE-2025-24813** não ocorre em uma instalação padrão do **Apache Tomcat**. Para que essa falha seja efetivamente explorável, é necessário que **determinadas condições estejam simultaneamente presentes no ambiente**, geralmente decorrentes de configurações incorretas, negligência no endurecimento do servidor ou decisões arriscadas durante o processo de deploy de aplicações *web*.

As principais condições que tornam um ambiente vulnerável são:

#### Permissão de escrita ativada no Default Servlet:

- Quando o parâmetro **readonly** é definido como *false* no arquivo de configuração **web.xml**, o Tomcat passa a aceitar requisições **HTTP** do tipo **PUT**, permitindo que arquivos sejam gravados diretamente no diretório da aplicação. Essa configuração, embora desativada por padrão, pode ser habilitada em ambientes que necessitam manipular uploads via métodos **HTTP** — o que, se não for bem controlado, abre caminho para que atacantes injetem arquivos maliciosos no servidor.

#### Suporte a partial PUT ativado:

- Por padrão, o Tomcat permite que arquivos sejam escritos em partes, utilizando cabeçalhos **HTTP** como **Content-Range**, possibilita que um invasor envie payloads maliciosos de forma fracionada, o que pode

dificultar a detecção por mecanismos de segurança e permitir a manipulação de arquivos já existentes.

#### Persistência de sessão baseada em arquivos ativada:

- Para que o ataque seja viável, a aplicação deve estar configurada para armazenar sessões de usuários em disco — ou seja, em arquivos locais. Essa abordagem, embora comum, pode criar um ponto de ataque se combinada com a capacidade de sobrescrever arquivos via PUT, especialmente arquivos de sessão válidos, o que poderia *levar à elevação de privilégios ou execução de código arbitrário*.

#### Presença de bibliotecas vulneráveis à desserialização:

- Mesmo que todas as condições anteriores estejam presentes, a execução efetiva do payload (isto é, a ativação do código malicioso) depende da presença de bibliotecas Java suscetíveis a *ataques de desserialização insegura*. O classpath da aplicação precisa incluir essas bibliotecas vulneráveis, como algumas versões conhecidas de frameworks e componentes que processam objetos serializados sem a devida validação, permitindo a execução de comandos arbitrários.

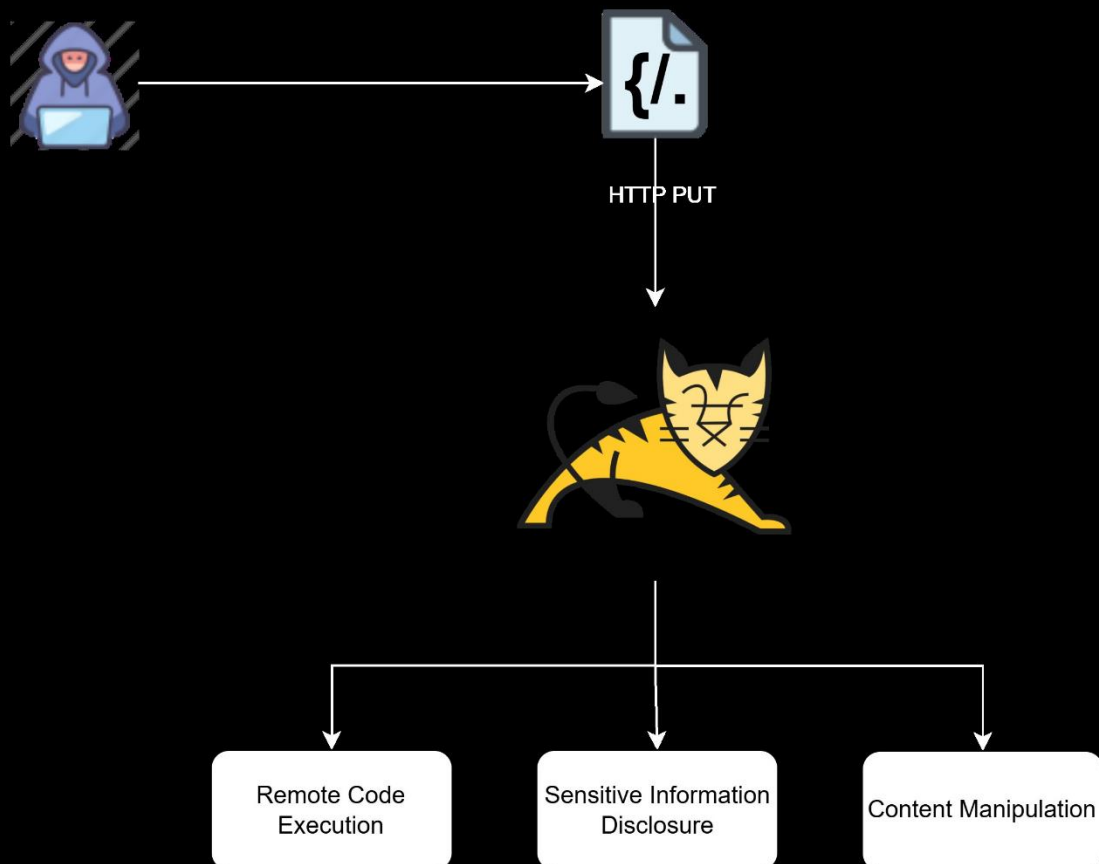


Figura 2 – Diagrama exploração Tomcat CVE-2025-24813.

### 3.3 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Initial Access	T1190 Exploit Public-Facing Application	A vulnerabilidade CVE-2025-24813 permite a exploração de aplicações Tomcat expostas à internet, possibilitando a execução remota de código (RCE) por meio de requisições HTTP do tipo PUT, em ambientes com configurações específicas habilitadas.

Tabela 1 – Tabela MITRE ATT&CK.

## 4 CONCLUSÃO

---

A **CVE-2025-24813** representa uma ameaça crítica à segurança de aplicações baseadas no Apache Tomcat, cuja exploração está diretamente ligada a configurações específicas que, se negligenciadas, expõem os servidores a ataques com alto impacto técnico e operacional. Quando explorada com sucesso, essa falha pode permitir a execução remota de código, comprometendo por completo a integridade e disponibilidade do ambiente afetado.

No entanto, os impactos vão além do aspecto técnico. Organizações que dependem de aplicações web para operações essenciais — como bancos, instituições de saúde, governo e educação — enfrentam riscos reais à **continuidade do negócio, perda de dados sensíveis, quebra de conformidade regulatória e danos à reputação institucional**. A presença da CVE-2025-24813 no catálogo KEV da CISA reforça a urgência de sua mitigação, sinalizando que a vulnerabilidade já está sendo explorada ativamente por agentes maliciosos.

Portanto, a resposta a essa vulnerabilidade deve ir além da correção técnica. É essencial que líderes de segurança e gestores de risco considerem essa ameaça como parte de uma estratégia ampla de **gestão de exposição**, com foco em resiliência cibernética, visibilidade contínua e alinhamento entre equipes técnicas e executivas.

## 5 RECOMENDAÇÕES

---

Conforme já citado neste relatório, a vulnerabilidade **CVE-2025-24813** afeta versões específicas do **Apache Tomcat** e pode permitir a execução remota de código (RCE), vazamento de informações sensíveis e injeção de conteúdo malicioso. Para mitigar os riscos associados a essa falha, são elencados abaixo pela ISH as seguintes recomendações:

### Atualizações de segurança

- Atualize o Apache Tomcat para as versões corrigidas:
  - Tomcat 11: Atualize para a versão 11.0.3 ou superior.
  - Tomcat 10.1: Atualize para a versão 10.1.35 ou superior.
  - Tomcat 9: Atualize para a versão 9.0.99 ou superior.

Para versões fora de suporte, como a série 8.5.x, é recomendado migrar para uma versão suportada, pois essas versões também podem ser vulneráveis.

### Configurações de mitigação

- Caso a atualização imediata não seja possível, considere as seguintes ações de mitigação:

Desabilitar escrita no Servlet Padrão:

- No arquivo web.xml, configure o parâmetro readonly como true para o servlet padrão, impedindo operações de escrita via requisições HTTP PUT.

Desabilitar suporte a Partial PUT:

- Configure o parâmetro allowPartialPut como false para evitar uploads parciais de arquivos, que podem ser explorados por atacantes.

Revisar persistência de sessão:

- Evite o uso de persistência de sessão baseada em arquivos, especialmente com o local de armazenamento padrão, pois isso pode ser explorado para execução de código malicioso.

Verificar bibliotecas de Desserialização:

- Analise as bibliotecas utilizadas pela aplicação para identificar possíveis vulnerabilidades de desserialização que possam ser exploradas em conjunto com essa falha.

### Medidas de segurança complementares

Restringir Métodos HTTP:

- Desabilite métodos HTTP não utilizados, como PUT e DELETE, para reduzir a superfície de ataque.

Implementar Firewall de Aplicação Web (WAF):

- Utilize um WAF para monitorar e bloquear requisições suspeitas que possam explorar essa vulnerabilidade.

Monitoramento Contínuo:

- Implemente sistemas de detecção de intrusões (IDS) e monitore logs do servidor para identificar atividades anômalas.

## 6 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- CTI Purple Team *by* ISH Tecnologia
- [NVD](#)
- [CISA-KEV](#)
- [MITRE ATT&CK](#)

## 7 AUTORES

---

- Gustavo Jatene de Oliveira – Threat Researcher
- Lucas Andrade Silva – Threat Researcher
- Ismael Rocha – Threat Intelligence Specialist



heimdall  
security research

A DIVISION OF ISH