

TLP: CLEAR



# BOLETIM DE SEGURANÇA

Falha de segurança no Apache Tomcat permite Execução Remota de Código (RCE)

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



ISH

### CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

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...

BAIXAR



ISH

### ALERTA PARA RETORNO DO MALWARE EMOTET!

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...

BAIXAR



ISH

### GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

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...

BAIXAR

## SUMÁRIO

1	Sumário Executivo .....	4
2	Informação sobre a vulnerabilidade.....	5
3	Recomendações.....	6
4	Referências .....	7
5	Autores.....	7

## 1 SUMÁRIO EXECUTIVO

---

A **Apache Software Foundation (ASF)** disponibilizou uma atualização de segurança para resolver uma vulnerabilidade no software de servidor **Tomcat**. A falha, identificada como [CVE-2024-56337](#), é uma mitigação incompleta de uma vulnerabilidade anterior, a [CVE-2024-50379](#), também encontrada no mesmo produto e corrigida anteriormente.

## 2 INFORMAÇÃO SOBRE A VULNERABILIDADE

---

As duas vulnerabilidades estão relacionadas a um tipo de **Time-of-check Time-of-use (TOCTOU) Race Condition**, que pode permitir a execução remota de código em sistemas de arquivos que não diferenciam letras maiúsculas de minúsculas. Isso ocorre quando o *servlet* padrão está configurado para permitir gravações.

O problema pode ser explorado por meio de leituras e uploads simultâneos do mesmo arquivo sob carga, o que pode contornar as verificações de diferenciação de maiúsculas e minúsculas realizadas pelo Tomcat, fazendo com que um arquivo carregado seja interpretado como um **Java Server Pages (JSP)** e, conseqüentemente, possibilitando a execução de código remoto. A **CVE-2024-56337** afeta as seguintes versões do Apache Tomcat:

- Apache Tomcat *11.0.0-M1* até *11.0.1* (corrigido na versão *11.0.2* ou posterior);
- Apache Tomcat *10.1.0-M1* até *10.1.33* (corrigido na versão *10.1.34* ou posterior);
- Apache Tomcat *9.0.0.M1* até *9.0.97* (corrigido na versão *9.0.98* ou posterior).

### 3 RECOMENDAÇÕES

---

Para minimizar os riscos relacionados à vulnerabilidade **CVE-2024-56337** no Apache Tomcat, é essencial realizar as **atualizações imediatas** para as versões corrigidas do software. Além disso, recomenda-se que os usuários implementem mudanças específicas na configuração, dependendo da versão do Java em uso:

- **Java 8** ou **Java 11**: Configurar explicitamente a propriedade do sistema `sun.io.useCanonCaches` como **false** (valor padrão é **true**);
- **Java 17**: Definir `sun.io.useCanonCaches` como **false**, caso já esteja configurada (o padrão é **false**);
- **Java 21** e **posteriores**: Nenhuma ação é necessária, pois a propriedade do sistema foi removida nessas versões.

## 4 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [NVD](#)
- [CWE](#)
- [Thehackernews](#)

## 5 AUTORES

---

- Rafael de Moura Salomé



heimdall  
security research

A DIVISION OF ISH