TLP: CLEAR

BOLETIM DE SEGURANÇA

Exploração de vulnerabilidade no Apache Struts2 permite envio de cargas maliciosas

heimdall
security research

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 TABELAS

1 SUMÁRIO EXECUTIVO

Atores maliciosos iniciaram a exploração de uma nova vulnerabilidade identificada no **Apache Struts2**, uma popular estrutura de código aberto utilizada no desenvolvimento de aplicativos web em Java. Classificada como crítica, essa falha de segurança, registrada sob o identificador **CVE-2024-53677**, apresenta um alto potencial de causar impactos severos caso não seja corrigida prontamente.

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

Recentemente, o **Apache Struts2** revelou uma vulnerabilidade crítica, destacando que ela está relacionada a ataques de "***path traversal***" (**travessia de diretórios**). Essa falha permite que invasores enviem arquivos para locais que deveriam ser inacessíveis, possibilitando a execução remota de código. Caso consigam carregar um webshell na raiz do servidor web, os invasores podem obter controle não autorizado sobre o sistema comprometido. Essa vulnerabilidade parece estar associada a uma falha anterior, registrada como **CVE-2023-50164**, cuja correção foi insuficiente, resultando no problema atual. Apesar das ações do Apache, a mitigação dessa vulnerabilidade é desafiadora. A organização recomenda que os usuários migrem para um novo mecanismo de **Action File Upload**, já que o mecanismo antigo deixa os sistemas expostos a ataques.

Explorações de **Prova de Conceito (PoC)** para a vulnerabilidade **CVE-2024-53677** já foram publicadas, e diversos ataques têm sido realizados com base nesses códigos, visando identificar sistemas vulneráveis. Esses ataques frequentemente utilizam solicitações *HTTP POST* para carregar arquivos maliciosos, como o "*exploit.jsp*", um script simples projetado para verificar se o **Apache Struts** está presente. Se o carregamento for bem-sucedido, os invasores podem localizar o script por meio de solicitações *HTTP GET* e realizar atividades maliciosas de forma remota.

Abaixo está um exemplo de um código de exploração.

```
POST /actionFileUpload HTTP/1.1
Host: [honeypot IP address]:8090
User-Agent: python-requests/2.32.3
Accept-Encoding: gzip, deflate, zstd
Accept: */*
Connection: keep-alive
Content-Length: 222 Content-Type: multipart/form-data;
boundary=0abcfc26e3fa0afbd6db1ba369dfcc37 --
0abcfc26e3fa0afbd6db1ba369dfcc37
Content-Disposition: form-data; name="file"; filename="exploit.jsp"
Content-Type: application/octet-stream <% out.println("Apache
Struts"); %> --0abcfc26e3fa0afbd6db1ba369dfcc37--*** su
```

Tabela 1 – Exemplo de comando utilizado.

3 RECOMENDAÇÕES

Dada a gravidade dessa vulnerabilidade, é essencial que as organizações que utilizam o **Apache Struts2** atualizem seus sistemas com a máxima urgência. Recomenda-se também a adoção do novo mecanismo **Action File Upload** que é uma medida indispensável para reforçar a segurança. Paralelamente, é importante realizar um monitoramento constante do tráfego de rede em busca de atividades anômalas ou não autorizadas, o que pode auxiliar na identificação e contenção de possíveis ameaças.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Struts**
- **ISC SANS**
- **NVD**
- **GBHackers**

5 AUTORES

- **Rafael de Moura Salomé**

heimdall
security research
A DIVISION OF ISH