Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

Alerta nº 05/2017 – Vulnerabilidade Apache Struts com o plugin REST (CVE-2017-9805)

1. Descrição do Problema

Foi descoberta uma vulnerabilidade crítica que afeta versões do Apache Struts. A vulnerabilidade pode permitir a execução remota de comandos no servidor.

Em 5 de setembro de 2017, pesquisadores da "lgtm", encontraram uma vulnerabilidade que está relacionada com a forma insegura de desserialização de dados realizada pelo framework. Dados originados em fontes não confiáveis, tais como formulários HTTP ou outras conexões (sockets), podem ser "convertidos" em objetos Java, o que possibilita a execução de código malicioso por um atacante.

https://lgtm.com/blog/apache_struts_CVE-2017-9805_announcement,

2. Versões afetadas

A vulnerabilidade afeta aplicações que utilizam o framework Apache Struts com o plugin REST nas versões Struts 2.1.2 até Struts 2.3.33 e Struts 2.5 até Struts 2.5.12.

3. Sugestões para Mitigação do Problema

De acordo com o security bulletin do projeto Apache Struts em https://cwiki.apache.org/confluence/display/WW/S2-052, a recomendação para correção da vulnerabilidade é a atualização para a versão 2.5.13. Caso não seja possível realizar a atualização de imediato, a recomendação é que o plugin REST seja removido ou tenha sua utilização limitada para páginas normais do servidor e no modo JSON apenas, conforme configuração a seguir:

3.1. Desabilitar páginas XML e requisições para essas páginas:

"<constant name="struts.action.extension" value="xhtml,,json" />"

3.2. Sobrescrever getContentType em XStreamHandler:

```
public class MyXStreamHandler extends XStreamHandler { public String getContentType() {
 return "not-existing-content-type-@;/&%$#@";
 }
}
```

3.3. Registrar o handler sobrescrevendo-o pelo que é fornecido pelo framework em struts.xml:

<bean type="org.apache.struts2.rest.handler.ContentTypeHandler" name="myXStreamHandmer" class="com.company.MyXStreamHandler"/>

<constant name="struts.rest.handlerOverride.xml" value="myXStreamHandler"/>

Os detalhes técnicos da vulnerabilidade podem ser encontrados no link https://lgtm.com/blog/apache_struts_CVE-2017-9805.

Referências:

- https://lgtm.com/blog/apache_struts_CVE-2017-9805_announcement
- https://cwiki.apache.org/confluence/display/WW/S2-052
- https://lgtm.com/blog/apache_struts_CVE-2017-9805

Brasília-DF, 16 de outubro de 2017.

Equipe do CTIR Gov