2022-06-03 - CVE-2022-26134- 远程代码执行漏洞安全风险

主题	CVE-2022-26134- -unauthenticated remote code execution vulnerability
公告发布日期	2022-06-02

影响产品	• Confluence
	  • Confluence Server
	  • Confluence Data Center

CVE ID	CVE-2022-26134
影响版本	所有版本
修复版本	• 7.4.17 • 7.13.7 • 7.14.3 • 7.15.2 • 7.16.4 • 7.17.4 • 7.18.1

说明

在Atlassian Confluence Server and Data Center中存在ONGL注入漏洞，未经身份验证的远程攻击者可以利用该漏洞在Atlassian Confluence Server and Data Center上注入恶意ONGL表达式，造成任意代码执行并部署WebShell。

Atlassian建议升级到最新的长期支持版本。

注意：如果在集群中运行Confluence，则在没有停机的情况下无法升级到固定版本，也称为滚动升级。按照升级Confluence Data Center中的步骤操作。

临时修补

对于Confluence7.X版本，如果不进行升级到长期支持版本，可以通过以下策略进行临时性的修补。

针对Confluence 7.15.0 - 7.18.0之间的版本

- 关闭Confluence
- 在https://packages.atlassian.com/maven-internal/opensymphony/xwork/1.0.3-atlassian-10/xwork-1.0.3-atlassian-10.jar 下载到服务器上
- 删除或者将<confluence-install>/confluence/WEB-INF/lib/xwork-1.0.3-atlassian-8.jar 移出Confluence 安装目录
- 将第二步下载的文件复制到<confluence-install>/confluence/WEB-INF/lib/ 目录中
- 检查该文件权限是否和所在目录的其他文件权限一致。
- 启动Confluence

针对 Confluence 7.0.0 - Confluence 7.14.2

- 关闭Confluence
- 将以下三个文件下载到服务器
    - https://packages.atlassian.com/maven-internal/opensymphony/xwork/1.0.3-atlassian-10/xwork-1.0.3-atlassian-10.jar
    - https://packages.atlassian.com/maven-internal/opensymphony/webwork/2.1.5-atlassian-4/webwork-2.1.5-atlassian-4.jar
    - https://confluence.atlassian.com/doc/files/1130377146/1137639562/3/1654274890463/CachedConfigurationProvider.class
- 删除或者移出以下路径的文件
    - <confluence-install>/confluence/WEB-INF/lib/xwork-1.0.3.6.jar
    - <confluence-install>/confluence/WEB-INF/lib/webwork-2.1.5-atlassian-3.jar
- 将下载的xwork-1.0.3-atlassian-10.jar复制到<confluence-install>/confluence/WEB-INF/lib/
- 将下载的webwork-2.1.5-atlassian-4.jar复制到<confluence-install>/confluence/WEB-INF/lib/
- 检查上述文件权限是否和同一目录的其他文件权限一样。
- 切换到目录<confluence-install>/confluence/WEB-INF/classes/com/atlassian/confluence/setup
    - 新建目录webwork
    - 将下载的CachedConfigurationProvider.class复制到<confluence-install>/confluence/WEB-INF/classes/com/atlassian/confluence/setup/webwork目录中
    - 确保复制的文件和新建的目录所有权等权限匹配
- 启动Confluence

提醒

- 如果在集群内运行Confluence则需要在每个节点上重复以上过程
- 如果使用是的Confluence6版本，请进行产品升级

针对Confluecne6.X处理

我们可以对Confluence6.x版本进行URL的拦截进行处理，主要策略是检查请求的URL路径，并进行拒绝服务。

如我们使用的是nginx前端，可以进行以下脚本上的配置

```
server {
  listen    80;
  server_name domain.cn;
  location / {
    if ($request_uri ~ "*/WEB-INF/*") { ## 对包括请求URL 地址包括/WEB-INF/的请求，进行拦截，返回404提示未找到
      return 404;
    }
    proxy_redirect off;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_pass  http://confluence;
  }

  error_page  500 502 503 504 /50x.html;

}
```

File	Modified
File 验证脚本-CVE-2022-26134	2022-06-08 by 红旗公