[安全通知] 关于 AAS 2018 年安全补丁更新说明

尊敬的客户：

您好，近日，我方根据最新官方公布的漏洞，检查了我方的产品，攻击者可利用漏洞实施权限提升、远程代码执行等攻击。

为避免您的业务受影响，建议您及时开展安全自查，如在受影响范围，请您及时进行更新修复，避免被外部攻击者入侵。

漏洞详情列表如下：

openssh

CVE-2018-15473

OpenSSH7.7 以及之前版本容易出现用户枚举漏洞，因为在完全解析包含请求的数据包之后，不会延迟对无效身份验证用户的救助，这与 auth2-gss.c，auth2-hostbased.c 和 auth2-pubkey .c 有关

CVE-2017-15906

在 7.6 之前的 OpenSSH 中的 sftp-server.c 中的 process_open 函数不能正确地防止以只读模式执行写操作，这允许攻击者创建零长度文件。

Apache Struts

CVE-2018-11776

当 alwaysSelectFullNamespace 为 true（由用户或像插件插件这样的插件）时，Apache Struts 版本 2.3 到 2.3.34 和 2.5 到 2.5.16 可能会遇到远程执行代码，然后：结果使用没有

命名空间，同时， upper package 没有或者是 wildcard 命名空间，与结果类似，当使用没有值和动作集的 url 标签时同样的可能性，同时它的上层包没有或通配符命名空间。

CVE-2017-9805

Apache Struts 2.1.2 到 2.3.34 之前的 2.3.x 和 2.5.13 之前的 2.5.x 中的 REST 插件的 XStream 组件存在反序列化漏洞，使用带有 XStream 实例的 XStreamHandler 进行反序列化操作时，未对数据内容进行有效验证，存在安全隐患，可被远程攻击。

Apache tomcat

CVE-2018-8037

如果应用程序在容器触发异步超时的同时完成异步请求，则存在竞争条件，这可能导致用户看到针对不同用户的响应。 NIO 和 NIO2 连接器中存在另一个问题，即当应用程序完成异步请求并且容器同时超时时，它们无法正确跟踪连接的关闭。 这也可能导致用户看到针对另一个用户的响应。 受影响的版本：Apache Tomcat 9.0.0.M9 到 9.0.9 和 8.5.5 到 8.5.31。

CVE-2018-1336

在具有补充字符的 UTF-8 解码器中不正确地处理溢出可能导致解码器中的无限循环导致拒绝服务。 受影响的版本：Apache Tomcat 9.0.0.M9 到 9.0.7,8.5.0 到 8.5.30,8.0.0.RC1 到 8.0.51 和 7.0.28 到 7.0.86。

CVE-2018-1305

Apache Tomcat 9.0.0.M1 到 9.0.4,8.5.0 到 8.5.27,8.0.0.RC1 到 8.0.49 和 7.0.0 到 7.0.84 中 Servlet 注释定义的安全性约束仅适用于 Servlet 已加载。 因为以这种方式定义的安全性约束适用于 URL 模式以及该点下面的任何 URL，所以可能 - 根据 Servlet 的加载顺序 - 可能会出现一些不应用的安全性约束。 这可能会向未授权访问它们的用户公开资源。

CVE-2018-1304

在 Apache Tomcat 9.0.0.M1 到 9.0.4,8.5.0 到 8.5.27,8.0.0.RC1 到 8.0 中未正确处理精确映射到上下文根的“”（空字符串）的 URL 模式 当用作安全约束定义的一部分时，.49 和 7.0.0 到 7.0.84。 这导致约束被忽略。 因此，未经授权的用户可以访问本应受到保护的 Web 应用程序资源。 只有空字符串的 URL 模式的安全性约束受到影响。

【影响版本】

目前已知受影响产品如下：

AAS4.8.6 AAS5.0

【修复建议】

1，将 openssh 升级到 7.8 （点击下载）

2，将 struts 升级到 2.3.35 （点击下载）

3，将 tomcat 升级到 8.5.33 （点击下载）

请下载最新安全补丁进行更新