INFORS 中创中间件

中创应用服务器

安全手册

山东中创软件商用中间件股份有限公司

2022 年 09 月

目　录

1 安全须知

首先，感谢您使用我司中创应用服务器软件产品（InforSuite AS）。

依据《中华人民共和国网络安全法》要求，为切实保障网络安全，落实网络安全责任，建议您在首次使用中创应用服务器产品时，需要格外注意以下四个方面：

1.排查并解决三员管理弱口令等安全隐患。针对产品中管理员（admin 或 inforsAdmin）、安全员（securityUser）、审计员（auditUser）三员账户口令，须根据要求设定符合强度要求的密码，且定期进行更换，确保无默认口令、空口令、弱口令和长期不变口令等情况的发生。

2.限制中间件产品管理工具可访问权限及范围。建议将中创应用服务器产品的管理工具端口（默认端口为 8060，以实际使用端口为准）控制在贵单位局域网管理员所在网段范围内访问，不对外暴露管理工具访问端口，以保障运行环境安全稳定运行。如需要暴露端口，务必采用一定手段进行管控，如白名单等。

3.使用新建域。在生产环境中，建议首次启动产品时，使用命令生成新的域，不使用产品自带的默认域。

4.请及时参照我司网站中对应产品漏洞修复声明并下载补丁进行更新。产品补丁发布地址为： https://www.inforbus.com/upgrade.html。

2 常见安全问题解决方案

2.1 用户口令管理

2.1.1 用户名口令修改

首次登陆时，产品中的管理员（admin 或 inforsAdmin）、安全员（securityUser）、审计员（auditUser）三员账户口令均默认为 Cvicse@as123，登陆成功后，请根据提示立即修改默认口令。或到“域”→“管理员口令”下修改当前管理员用户口令。修改其他身份用户的口令时需要使用安全员用户登录管理控制台，在用户管理页面可对管理员用户和审计员用户的口令进行重置，可以修改安全员用户口令。

强度须满足：大写字母、小写字母、数字、特殊符号（~！@#￥%^*()_）四种类型至少三种组混编，且不少于 8 位。密码规则在 domain.xml 中进行定义，可以手动进行修改。记录用户最近使用的 3 次口令，新口令不能与最近 3 次使用的口令一致。

注意：10.5.1 版本可修改自己的口令。

2.1.2 创建域

产品安装成功后，首次启动服务器时使用命令创建新的域，可以保障密钥对的唯一性，从而在使用 https 安全协议进行访问时保证通信安全。

一般情况下，通过执行 asadmin.sh 来启动服务器。打开命令窗口，进入 AppServer/bin 目录，输入 asadmin.sh，按回车键，若是首次启动，出现如下信息，表明执行成功：

```
Domains do not exist in this AS,you need to create production domain(P) or test domain(T).Please chose P/T:
```

根据实际情况选择模板创建域，其中 T 为测试域，P 为生产域。

注意：windows 环境通过执行 asadmin.bat 脚本启动中创应用服务器。

2.1.3 登录失败锁定

设置登录失败锁定需要使用安全员（securityUser）登录管理控制台（https://IP:Port）进行操作。登录安全员管理界面，改密码有效期、错误次数、锁定时间，点击“登录配置”

保存。

2.2 SSL/TLS 相关漏洞

中创应用服务器 https 通信协议默认有密码套件加密设置，在进行安全扫描时可能会扫出存在漏洞的密码套件，此时可将存在安全问题的密码套件排除掉，使用有效的密码套件进行加密处理。

前置处理步骤为：

登录管理控制台（https://IP:Port）操作，

“配置管理”→“server-config”→“网络配置”→“协议”→“http-listener-1”→ “SSL”、

“配置管理”→“server-config”→“网络配置”→“协议”→“http-listener-2”→ “SSL”

2.2.1 安全漏洞扫描中提示有SSL漏洞Factoring RSA Export Keys

处理步骤：

分别对两个页面中的密码套件进行配置，设置 SSL 采用高版本的加密算法 TLS，重启服务器生效。

（1）在上述两个 SSL 界面中同时设置 SSL3 不启用，启动 TLS 如下（证书昵称为填写：s1as）

（2）选择设置所选常用密码套件为：TLS_RSA_WITH_AES_128_CBC_SHA；

（3）选择设置所选 Ephemeral Diffie-Hellman 密码套件为：

TLS_DHE_RSA_WITH_AES_128_CBC_SHA 和 TLS_DHE_DSS_WITH_AES_128_CBC_SHA

2.2.2 SSL/TLS LogJam中间人安全限制绕过漏洞 (CVE-2015-4000)

处理步骤：

在上述两个 SSL 界面中密码套件中排除包含 EXPORT 或者 EXP 的算法的套件，重启服务器生效。

2.2.3 SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱

处理步骤：

在上述两个 SSL 界面中密码套件中排除包含 DH 算法的套件，重启服务器生效。

2.2.4 SSL 3.0 POODLE攻击信息泄露漏洞(CVE-2014-3566)

处理步骤：

在上述两个 SSL 界面中禁用 SSL3.0，即取消勾选 SSL3.0，重启服务器生效。

2.2.5 SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)

处理步骤：

在上述两个 SSL 界面中禁用 RC4，如下图配置，重启服务器生效。

2.2.6 Sec-admin-listener端口漏洞修改

在上述两个 SSL 界面中的可用的常用密码套件中选择 TLS_RSA_WITH_AES_128_CBC_SHA ，重启服务器生效。

2.2.7 开启TLS1.2 协议

在上述两个 SSL 界面取消 TLS、TLS1.1、启用的勾选框，只勾选 TLS1.2 的勾选框，保存。

注意：jdk1.7 默认支持 tls1 ，如果要在 jdk1.7 上开启 TLS1.2 的支持。需要做以下操作：

方案 1：需要在 JVM 参数添加：-Dhttps.protocols=TLSv1.1,TLSv1.2 。

方案 2：升级版本到 jdk1.8， jdk1.8 默认支持 tls1.2。

2.3 HTTP 相关配置

HTTP 相关配置前置操作步骤：

登录管理控制台（https://IP:Port）操作，

“配置管理”→“server-config”→“网络配置”→“协议”→“http-listener-1”→ “HTTP”、

“配置管理”→“server-config”→“网络配置”→“协议”→“http-listener-2”→ “HTTP”

2.3.1 提升HTTP安全级别

HTTP1.0 定义了三种请求方法： GET， POST 和 HEAD 方法；HTTP1.1 新增了五种请求方法：OPTIONS，PUT，DELETE，TRACE 和 CONNECT 方法。

若在安全扫描中提示启用了不安全的 http 方法，在上述两个 HTTP 界面的填写“禁止 HTTP 访问方式”的输入框中填写要禁用的 HTTP 访问方式，保存后重启服务器生效。

2.3.2 Slow HTTP Denial of Service Attack问题

"http 慢速拒绝攻击"的问题可通过调整超时时间和请求超时时间解决，

超时时间默认时间为 30s，可调整为 10s 测试。

请求超时默认时间为 900s，可调整为 10s 测试。（此项可不作调整）

在上述两个 HTTP 界面将“超时时间”改为 10s，“请求超时时间”修改为 10s，重启生效。

2.3.3 中创应用服务器X-powered-By显示Servlet和jsp版本信息

攻击者在获得中间件版本信息后，可针对新的寻找当前版本中间件存在的安全漏洞，进而进行有针对性的工具，我们通过屏蔽 Xpowered By 的信息解决该问题。

在上述两个 HTTP 界面将“XPowered By”的启用勾选去掉。修改保存后重启应用服务器生效。

2.4 应用开启 https 协议支持

需要登录管理控制台（https://IP:Port）操作：

“配置管理”->”server-config”-> “网络配置” -> “网络监听程序” -> “http-listener-2”，在编辑网络监听程序页面，勾选“状态”的复选框，点击保存，开启 https 协议支持。

2.5 登录资源限制

需要登录管理控制台（https://IP:Port）操作：

“配置管理”->”server-config”->“虚拟服务器”->“server”，在远程访问模块，在“禁止远程访问 IP 地址”文本框中填入远程客户机 IP 地址。多个 IP 之间用逗号隔开。

2.6 JMX 反序列化漏洞

处理步骤：

1. 登录 InforSuite AS 管理控制台，进入“配置管理”→ “server-config”→“JVM 设置”

2. 点击“添加 JVM 选项”，添加内容：

-Dcom.sun.management.jmxremote.authenticate=true

-Dcom.sun.management.jmxremote.ssl=true

2.7 开启安全管理域后浏览器访问不到报弱临时 Diffie-Hellman 密钥

采用 https 协议访问应用，发现 IE、360 浏览器可以访问，火狐和谷歌浏览器不能访问，报如下错误：安全连接失败 连接 192.168.0.211:8181 时发生错误。在服务器密钥交换握手信息中 SSL 收到一个弱临时 Diffie-Hellman 密钥。（错误码：ssl_error_weak_server_ephemeral_dh_key）

处理步骤：

1、谷歌浏览器：在谷歌浏览器的快捷方式后面加加粗部分如下所示：

“C:\Users\Administrator\AppData\Local\Google\Chrome\Application\chrome.exe” **--cipher-suite-blacklist=0x0039,0x0033**

注意：在“...\Application\chrome.exe”后有一个空格

2、火狐浏览器则需要安装“Disable DHE”插件。

2.8 请求缺少 X-Content-Type-Options， X-XSS-Protection，Content-Security-Policy 头

该问题可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置，可能会获取初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息。

解决方案：

在 default-web.xml（\as\domains\domain1\config）中添加过滤器配置，

```
<filter>
    <filter-name>httpHeaderSecurityFilter</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter
</filter-class>
    <init-param>
<param-name>blockContentTypeSniffingEnabled</param-name>
        <param-value>true</param-value>
    </init-param>
    <init-param>
        <param-name>xssProtectionEnabled</param-name>
        <param-value>true</param-value>
    </init-param>
    <init-param>
        <param-name>contentSecurityPolicyEnabled</param-name>
        <param-value>true</param-value>
    </init-param>
    <init-param>
        <param-name>hstsEnabled</param-name>
        <param-value>false</param-value>
    </init-param>
    <init-param>
        <param-name>antiClickJackingEnabled</param-name>
        <param-value>false</param-value>
    </init-param>
</filter>
<filter-mapping>
    <filter-name>httpHeaderSecurityFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

此五项属性默认都为 true，若要关闭可设置为 false。其中标红的两项影响到管理控制台登录，因此设置为 false。