奇安信
新一代网络安全领军者

Oracle 多个组件漏洞

安全风险通告

奇安信 CERT

2022 年 04 月 20 日

修订历史

时间	更新内容
2022 年 04 月 20 日	监测到 Oracle 官方发布安全更新，发布安全风险通告。

目录

第1章 安全通告

尊敬的客户：

Oracle 官方发布了 2022 年 4 月的关键安全补丁集合更新 CPU（Critical Patch Update），修复了多个存在于 WebLogic 中的漏洞包括 CVE-2022-23305、CVE-2022-21420、CVE-2022-21441、CVE-2022-23437、CVE-2022-21453、CVE-2021-41184。

经过技术研判，奇安信 CERT 认为 CVE-2022-23305（Oracle WebLogic Server 远程代码执行漏洞）、CVE-2022-21420（Oracle Coherence 远程代码执行漏洞）漏洞利用限制较少，影响较为严重。**鉴于漏洞危害性较大，奇安信 CERT 建议客户尽快应用本次关键安全补丁集合（CPU）**。

奇安信 CERT 将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

第2章 漏洞信息

Oracle 官方发布了 2022 年 04 月的关键补丁程序更新 CPU（Critical Patch Update），其中修复了多个存在于 WebLogic 中的漏洞

漏洞名称	**Oracle WebLogic Server 远程代码执行漏洞**		
公开时间	2022-01-18	**更新时间**	2022-04-20
CVE 编号	CVE-2022-23305	**其他编号**	QVD-2022-1142
威胁类型	代码执行	**技术类型**	SQL 注入
厂商	Oracle	**产品**	WebLogic Server
风险等级			
奇安信 CERT 风险评级		**风险等级**	
高危		蓝色（一般事件）	
现时威胁状态			
POC 状态	**EXP 状态**	**在野利用状态**	**技术细节状态**
未公开	未公开	未发现	未公开
漏洞描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中引用了第三方依赖 Apache Log4j，允许未经身份验证的攻击者通过 HTTP 访问服务器，成功利用此漏洞可导致 Oracle WebLogic Server 被接管。		
影响版本	12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0		
其他受影响组件	Apache Log4j 1.2.x（该版本已停止维护）		

漏洞名称	**Oracle Coherence 远程代码执行漏洞**		
公开时间	2022-04-20	更新时间	2022-04-20
CVE 编号	CVE-2022-21420	其他编号	QVD-2022-1902
威胁类型	代码执行	技术类型	不可信数据的反序列化
厂商	Oracle	产品	Coherence
风险等级			
奇安信 CERT 风险评级		风险等级	
高危		蓝色（一般事件）	
现时威胁状态			
POC 状态	EXP 状态	在野利用状态	技术细节状态
未公开	未公开	未发现	未公开
漏洞描述	Oracle Coherence 中存在远程代码执行漏洞，允许未经身份验证的攻击者通过 T3 访问服务器来破坏 Oracle Coherence，成功利用此漏洞可接管 Oracle Coherence。		
影响版本	12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0		
其他受影响组件	无		

漏洞名称	**Oracle WebLogic Server 拒绝服务漏洞**		
公开时间	2022-04-20	更新时间	2022-04-20
CVE 编号	CVE-2022-21441	其他编号	QVD-2022-1903
威胁类型	拒绝服务	技术类型	不可信数据的反序列化
厂商	Oracle	产品	WebLogic Server

风险等级			
奇安信 CERT 风险评级		风险等级	
高危		蓝色（一般事件）	
现时威胁状态			
POC 状态	EXP 状态	在野利用状态	技术细节状态
未公开	未公开	未发现	未公开
漏洞描述	Oracle WebLogic Server 的 Core 中存在漏洞，允许未经身份验证的攻击者通过 T3/IIOP 访问服务器来攻击 Oracle WebLogic Server，成功利用此漏洞可能会导致 Oracle WebLogic Server 挂起或 DOS。		
影响版本	12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0		
其他受影响组件	无		

漏洞名称	Oracle WebLogic Server 拒绝服务漏洞		
公开时间	2022-01-24	更新时间	2022-04-20
CVE 编号	CVE-2022-23437	其他编号	QVD-2022-1904
威胁类型	拒绝服务	技术类型	XML 注入
厂商	Oracle	产品	WebLogic Server
风险等级			
奇安信 CERT 风险评级		风险等级	
中危		蓝色（一般事件）	
现时威胁状态			
POC 状态	EXP 状态	在野利用状态	技术细节状态

未公开	未公开	未发现	未公开
漏洞描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中引用了第三方工具 Apache Xerces-J，允许未经身份验证的攻击者通过 HTTP 访问来攻击 Oracle WebLogic Server，此攻击需要与受害者进行交互，成功利用此漏洞可能会导致 Oracle WebLogic Server 挂起或 DOS。		
影响版本	12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0		
其他受影响组件	Apache XercesJ <= 2.1.2		

漏洞名称	**Oracle WebLogic Server 身份验证绕过漏洞**		
公开时间	2022-04-20	**更新时间**	2022-04-20
CVE 编号	CVE-2022-21453	**其他编号**	QVD-2022-1905
威胁类型	身份验证绕过	**技术类型**	未授权访问
厂商	Oracle	**产品**	WebLogic Server
风险等级			
奇安信 CERT 风险评级		**风险等级**	
中危		蓝色（一般事件）	
现时威胁状态			
POC 状态	**EXP 状态**	**在野利用状态**	**技术细节状态**
未公开	未公开	未发现	未公开
漏洞描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中存在漏洞，允许未经身份验证的攻击者通过 HTTP 访问来攻击 Oracle WebLogic Server，此攻击需要与受害者进行交互，此漏		

	洞可能会影响其他产品，成功利用此漏洞可能导致对某些 Oracle WebLogic Server 可访问数据的未授权更新、插入或删除。
影响版本	12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0
其他受影响组件	无

漏洞名称	**Oracle WebLogic Server 身份验证绕过漏洞**		
公开时间	2022-04-20	**更新时间**	2022-04-20
CVE 编号	CVE-2021-41184	**其他编号**	QVD-2021-25808
威胁类型	身份验证绕过	**技术类型**	跨站脚本攻击
厂商	Oracle	**产品**	WebLogic Server
风险等级			
奇安信 CERT 风险评级		**风险等级**	
中危		蓝色（一般事件）	
现时威胁状态			
POC 状态	**EXP 状态**	**在野利用状态**	**技术细节状态**
未公开	未公开	未发现	未公开
漏洞描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中存在漏洞，允许未经身份验证的攻击者通过 HTTP 访问来攻击 Oracle WebLogic Server，此攻击需要与受害者进行交互，此漏洞可能会影响其他产品，成功利用此漏洞可能导致对某些 Oracle WebLogic Server 可访问数据的未授权更新、插入或删除。		

影响版本	12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0
其他受影响组件	jQuery-UI <= 1.13.0

第3章 威胁评估

漏洞名称	Oracle WebLogic Server 远程代码执行漏洞		
CVE 编号	CVE-2022-23305	**其他编号**	QVD-2022-1142
CVSS 3.1 评级	高危	**CVSS 3.1 分数**	**9.8**
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	低	
	所需权限（PR）	**用户交互（UI）**	
	不需要	不需要	
	影响范围（S）	**机密性影响（C）**	
	不变	高	
	完整性影响（I）	**可用性影响（A）**	
	高	高	
危害描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中引用了第三方依赖 Apache Log4j，允许未经身份验证的攻击者通过 HTTP 访问服务器，成功利用此漏洞可导致 Oracle WebLogic Server 被接管。		

漏洞名称	Oracle Coherence 远程代码执行漏洞		
CVE 编号	CVE-2022-21420	**其他编号**	QVD-2022-1902
CVSS 3.1 评级	高危	**CVSS 3.1 分数**	**9.8**
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	低	
	所需权限（PR）	**用户交互（UI）**	
	不需要	不需要	

	影响范围（S）	**机密性影响（C）**
	不变	高
	完整性影响（I）	**可用性影响（A）**
	高	高
危害描述	Oracle Coherence 中存在远程代码执行漏洞，允许未经身份验证的攻击者通过 T3 访问服务器来破坏 Oracle Coherence，成功利用此漏洞可接管 Oracle Coherence。	

漏洞名称	Oracle WebLogic Server 拒绝服务漏洞		
CVE 编号	CVE-2022-21441	**其他编号**	QVD-2022-1903
CVSS 3.1 评级	高危	**CVSS 3.1 分数**	**7.5**
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	低	
	所需权限（PR）	**用户交互（UI）**	
	不需要	不需要	
	影响范围（S）	**机密性影响（C）**	
	不变	无	
	完整性影响（I）	**可用性影响（A）**	
	无	高	
危害描述	Oracle WebLogic Server 的 Core 中存在漏洞，允许未经身份验证的攻击者通过 T3/IIOP 访问服务器来攻击 Oracle WebLogic Server，成功利用此漏洞可能会导致 Oracle WebLogic Server 挂起或 DOS。		

漏洞名称	Oracle WebLogic Server 拒绝服务漏洞		
CVE 编号	CVE-2022-23437	**其他编号**	QVD-2022-1904
CVSS 3.1 评级	中危	**CVSS 3.1 分数**	**6.5**
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	低	
	所需权限（PR）	**用户交互（UI）**	
	不需要	需要	
	影响范围（S）	**机密性影响（C）**	
	不变	无	
	完整性影响（I）	**可用性影响（A）**	
	无	高	
危害描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中引用了第三方工具 Apache Xerces-J，允许未经身份验证的攻击者通过 HTTP 访问来攻击 Oracle WebLogic Server，此攻击需要与受害者进行交互，成功利用此漏洞可能会导致 Oracle WebLogic Server 挂起或 DOS。		

漏洞名称	**Oracle WebLogic Server 身份验证绕过漏洞**		
CVE 编号	CVE-2022-21453	**其他编号**	QVD-2022-1905
CVSS 3.1 评级	中危	**CVSS 3.1 分数**	**6.1**
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	低	
	所需权限（PR）	**用户交互（UI）**	
	不需要	需要	
	影响范围（S）	**机密性影响（C）**	

	改变	低
	完整性影响（I）	**可用性影响（A）**
	低	无
危害描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中存在漏洞，允许未经身份验证的攻击者通过 HTTP 访问来攻击 Oracle WebLogic Server，此攻击需要与受害者进行交互，此漏洞可能会影响其他产品，成功利用此漏洞可能导致对某些 Oracle WebLogic Server 可访问数据的未授权更新、插入或删除。	

漏洞名称	**Oracle WebLogic Server 身份验证绕过漏洞**		
CVE 编号	CVE-2021-41184	**其他编号**	QVD-2021-25808
CVSS 3.1 评级	中危	**CVSS 3.1 分数**	**6.1**
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	低	
	所需权限（PR）	**用户交互（UI）**	
	不需要	需要	
	影响范围（S）	**机密性影响（C）**	
	改变	低	
	完整性影响（I）	**可用性影响（A）**	
	低	无	
危害描述	Oracle Fusion Middleware 的 Oracle WebLogic Server 中存在漏洞，允许未经身份验证的攻击者通过 HTTP 访问来攻击 Oracle WebLogic Server，此攻击需要与受害者进行交互，此漏洞可能会影响其他产品，成功利用此漏洞可能导致对某些 Oracle WebLogic Server 可访问数据的未授权更新、插入或删除。		

第4章 处置建议

请参考以下链接尽快修复：

https://www.oracle.com/security-alerts/cpuapr2022.html

Oracle WebLogic Server 升级方式

1. Oracle WebLogic Server 11g：

bsu.cmd -install -patch_download_dir=C:\Oracle\Middleware\utils\bsu\cache_dir -patchlist=3L3H -prod_dir=C:\Oracle\Middleware\wlserver_10.3

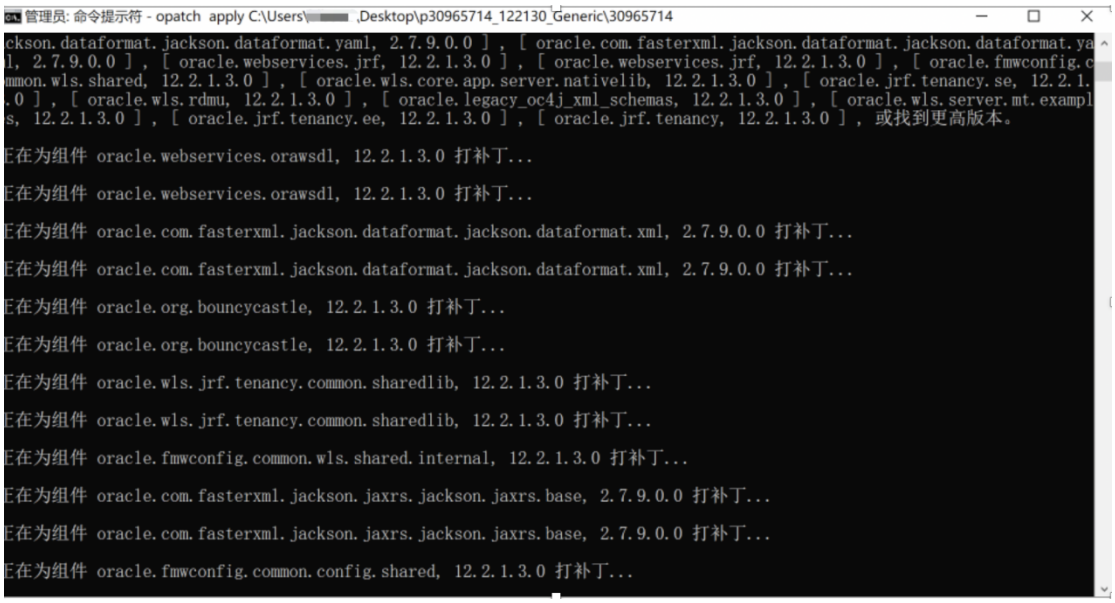
```
C:\Oracle\Middleware\utils\bsu>bsu.cmd -prod_dir=c:\Oracle\Middleware\wlserver_10.3 -status=applied -verbose -view
ProductName:       WebLogic Server
ProductVersion:    10.3 MP6
Components:        WebLogic Server/Core Application Server,WebLogic Server/Admi
                   nistration Console,WebLogic Server/Configuration Wizard and
                   Upgrade Framework,WebLogic Server/Web 2.0 HTTP Pub-Sub Serve
                   r,WebLogic Server/WebLogic SCA,WebLogic Server/WebLogic JDBC
                    Drivers,WebLogic Server/Third Party JDBC Drivers,WebLogic S
                   erver/WebLogic Server Clients,WebLogic Server/WebLogic Web S
                   erver Plugins,WebLogic Server/UDDI and Xquery Support,WebLog
                   ic Server/Evaluation Database,WebLogic Server/Workshop Code
                   Completion Support
BEAHome:           C:\Oracle\Middleware
ProductHome:       C:\Oracle\Middleware\wlserver_10.3
PatchSystemDir:    C:\Oracle\Middleware\utils\bsu
PatchDir:          C:\Oracle\Middleware\patch_wls1036
Profile:           Default
DownloadDir:       C:\Oracle\Middleware\utils\bsu\cache_dir
JavaVersion:       1.6.0_29
JavaVendor:        Sun


Patch ID:          3L3H
PatchContainer:    3L3H.jar
Checksum:          1872068379
Severity:          optional
Category:          General
CR/BUG:            30109677
Restart:           true
Description:       WLS PATCH SET UPDATE 10.3.6.0.191015
WLS PATCH SET UPDATE 10
                   .3.6.0.191015



C:\Oracle\Middleware\utils\bsu>
```

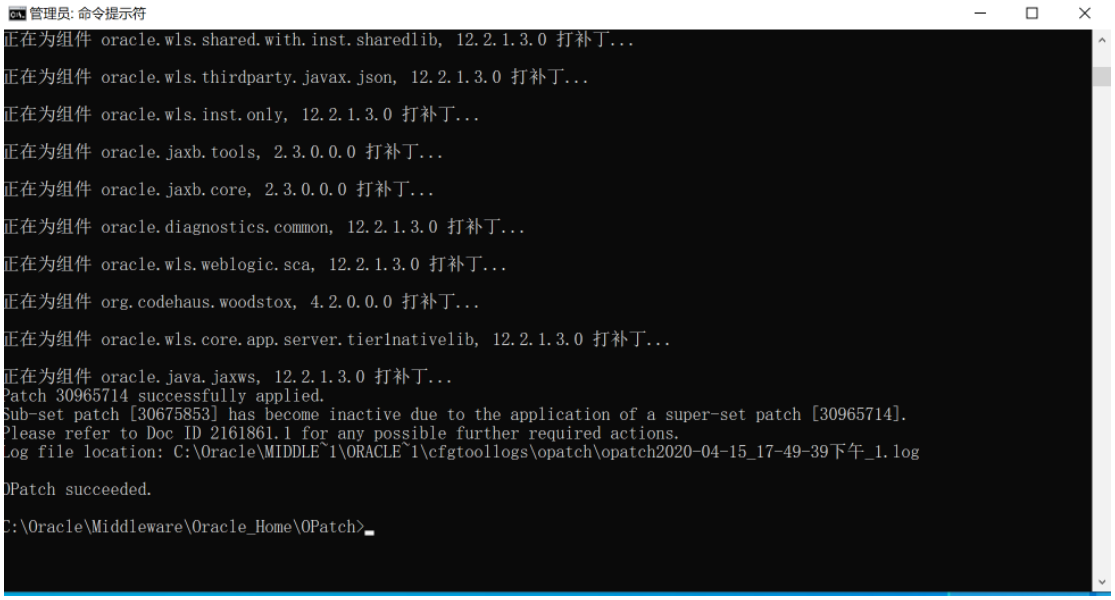
出现以上提示代表补丁安装成功。

2. Oracle WebLogic Server 12c：

使用 opatch apply 安装补丁

C:\Oracle\Middleware\Oracle_Home\OPatch>opatch apply 本机补丁地址





注：补丁编号请自行更改为新补丁编号。

若非必须开启，请禁用 T3 和 IIOP 协议。

禁用 T3、IIOP 协议具体操作步骤如下：

1. 禁用 T3:

进入 WebLogic 控制台，在 base_domain 的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

在连接筛选器中输入：WebLogic.security.net.ConnectionFilterImpl，参考以下写法，在连接筛选器规则中配置符合企业实际情况的规则：

127.0.0.1 * * allow t3 t3s

本机 IP * * allow t3 t3s

允许访问的 IP * * allow t3 t3s

* * * deny t3 t3s

连接筛选器规则格式如下：target localAddress localPort action protocols，其中：

target 指定一个或多个要筛选的服务器。

localAddress 可定义服务器的主机地址。(如果指定为一个星号 (*)，则返回的匹配结果将是所有本地 IP 地址。)

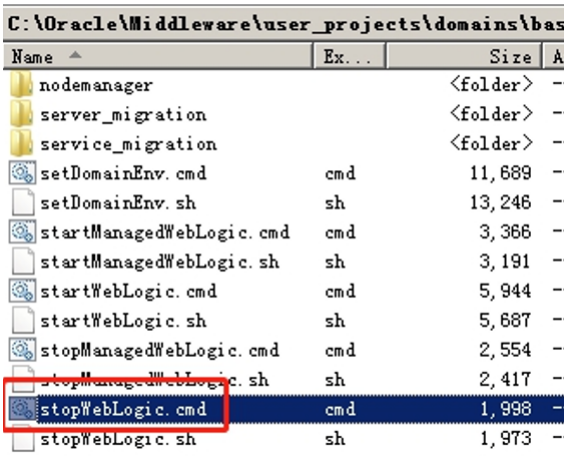
localPort 定义服务器正在监听的端口。(如果指定了星号，则匹配返回的结果将是服务器上所有可用的端口)。

action 指定要执行的操作。(值必须为“allow”或“deny”。)

protocols 是要进行匹配的协议名列表。(必须指定下列其中一个协议：http、https、t3、t3s、giop、giops、dcom 或 ftp。) 如果未定义协议，则所有协议都将与一个规则匹配。

保存后若规则未生效，建议重新启动 WebLogic 服务（重启 WebLogic 服务会导致业务中断，建议相关人员评估风险后，再进行操作）。以 Windows 环境为例，重启服务的步骤如下：

进入域所在目录下的 bin 目录，在 Windows 系统中运行 stopWebLogic.cmd 文件终止 WebLogic 服务，Linux 系统中则运行 stopWebLogic.sh 文件。



待终止脚本执行完成后，再运行 startWebLogic.cmd 或 startWebLogic.sh 文件启动 WebLogic，即可完成 WebLogic 服务重启。

2. 禁用 IIOP：

用户可通过关闭 IIOP 协议阻断针对利用 IIOP 协议漏洞的攻击，操作如下：

在 WebLogic 控制台中，选择“服务”->”AdminServer”->”协议”，取消“启用 IIOP”的勾选。并重启 WebLogic 项目，使配置生效。


ORACLE WebLogic Server® Administration Console
更改中心
查看更改和重新启动
启用配置编辑。将来在修改，添加或删除此域中的项目时，将自动激活这些更改。
域结构
base_domain
环境
部署
服务
安全领域
互用性
诊断
帮助主题
启用和配置 IIOP
配置定制网络通道
配置默认网络连接
系统状态
正在运行的服务器的健康状况
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
主页 注销 首选项 记录 帮助
欢迎, weblogic 连接到: base_domain
主页 >环境概要 >服务器概要 >AdminServer
消息
已激活所有更改。但是，要使这些更改生效，必须重新启动这 1 个项目。
设置更新成功。
AdminServer的设置
配置 协议 日志记录 调试 监视 控制 部署 服务 安全 注释
一般信息 HTTP jCOM IIOP 通道
保存
在此页中，您可以定义此服务器的 IIOP (Internet ORB 间协议) 设置。通过 IIOP，以不同编程语言编写的分布式程序可以通过 Internet 进行通信。
启用 IIOP
指定是否为此服务器的常规 (非 SSL) 和 SSL 端口都启用 IIOP 支持。 更多信息...
高级
保存

第5章 参考资料

[1] https://www.oracle.com/security-alerts/cpuapr2022.html

奇安信 CERT

【我们是谁】

奇安信应急响应部（又称：奇安信 CERT，奇安信 A-TEAM）成立于 2016 年，是属于奇安信旗下的网络安全应急响应平台，平台旨在第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案。

奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞，第一时间发布相关漏洞风险通告及可行的处置措施并获得官方致谢。欢迎有意者加入！

【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

【订阅方式】

发送接收邮箱和所属单位至：

cert@qianxin.com

【微信公众号】

奇安信 CERT