奇安信
新一代网络安全领军者

# GeoServer 远程代码执行漏洞

# (CVE-2024-36401)

# 安全风险通告

奇安信 CERT

2024 年 7 月 3 日

# 修订历史

| 时间 | 更新内容 |
| --- | --- |
| 2024 年 07 月 03 日 | 监测到官方修复 GeoServer 远程代码执行漏洞 (CVE-2024-36401)，该漏洞技术细节及 EXP 已公开，奇安信威胁情报中心安全研究员复现此漏洞。 |

# 文档信息

| | |
|---|---|
| **编号** | QiAnXinTI-QVD-2024-24967 |
| **事件性质** | 漏洞暴露事件 |
| **影响厂商** | 开源软件 |
| **影响产品** | GeoServer |
| **漏洞公开时间** | 2024 年 07 月 01 日 |
| **威胁类型** | 代码执行 |
| **利用可能性** | 高 |
| **发布日期** | 2024 年 07 月 03 日 |
| **更新日期** | 2024 年 07 月 03 日 |
| **风险等级** | 蓝色（一般事件） |
| **分析团队** | 奇安信威胁情报中心 |

# 目 录

**第一章 安全通告** . . . . . 1

**第二章 漏洞信息** . . . . . 2

**第三章 威胁评估** . . . . . 4

**第四章 处置建议** . . . . . 5

**第五章 产品解决方案** . . . . . 6

6.1 奇安信自动化渗透测试系统检测方案 . . . . . 6
6.2 奇安信开源卫士已支持 . . . . . 6
6.3 奇安信网神网络数据传感器系统产品检测方案 . . . . . 6
6.4 奇安信天眼产品解决方案 . . . . . 6
6.5 奇安信网站应用安全云防护系统已更新防护特征库 . . . . . 7

**第六章 参考资料** . . . . . 8

# 第一章 安全通告

尊敬的客户：

近日，奇安信 CERT 监测到官方修复 GeoServer 远程代码执行漏洞(CVE-2024-36401)，由于该系统不安全地将属性名称解析为 XPath 表达式，未经身份认证的远程攻击者可以通过该漏洞在服务器上执行任意代码，从而获取服务器权限。**目前该漏洞技术细节与 EXP 已在互联网上公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。**

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。

# 第二章 漏洞信息

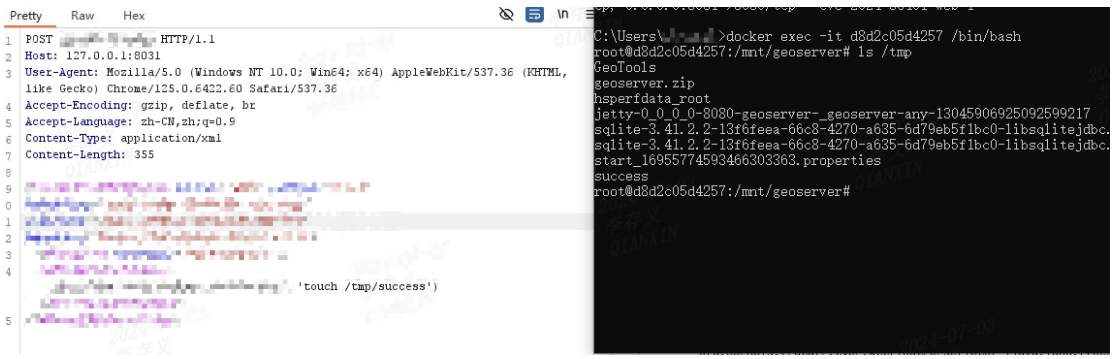
GeoServer 是一个开源的服务器软件，使用 Java 编写，主要功能是允许用户共享和编辑地理空间数据。它在设计时就考虑到了互操作性，支持使用开放标准来发布多种主流格式的空间数据。

近日，奇安信 CERT 监测到官方修复 GeoServer 远程代码执行漏洞(CVE-2024-36401)，由于该系统不安全地将属性名称解析为 XPath 表达式，未经身份认证的远程攻击者可以通过该漏洞在服务器上执行任意代码，从而获取服务器权限。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

| | | | |
|---|---|---|---|
| **漏洞名称** | GeoServer 远程代码执行漏洞 | | |
| **公开时间** | 2024-07-01 | **更新时间** | 2024-07-03 |
| **CVE 编号** | CVE-2024-36401 | **其他编号** | QVD-2024-24967<br>CNNVD-202407-085 |
| **威胁类型** | 代码执行 | **技术类型** | Eval 代码注入 |
| **厂商** | 开源软件 | **产品** | GeoServer |
| **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** |
| 已公开 | 已公开 | 未发现 | 已公开 |
| **漏洞成因** | GeoServer 调用的 GeoTools 库 API，在解析特性类型的属性/属性名称时，以不安全的方式将它们传递给 commons-jxpath 库，当解析 XPath 表达式时可以执行任意代码。 | | |

| | |
|---|---|
| **漏洞描述** | 由于该系统不安全地将属性名称解析为 XPath 表达式，未经身份认证的远程攻击者可以通过该漏洞在服务器上执行任意代码，从而获取服务器权限。 |
| **影响版本** | GeoServer < 2.23.6<br>2.24.0 <= GeoServer < 2.24.4<br>2.25.0 <= GeoServer < 2.25.2 |
| **其他受影响组件** | 无 |

目前，奇安信威胁情报中心安全研究员已成功复现 GeoServer 远程代码执行漏洞(CVE-2024-36401)，截图如下：




**鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。**

# 第三章 威胁评估

<table>
<tr><td>漏洞名称</td><td colspan="3">GeoServer 远程代码执行漏洞</td></tr>
<tr><td>CVE 编号</td><td>CVE-2024-36401</td><td>其他编号</td><td>QVD-2024-24967<br>CNNVD-202407-085</td></tr>
<tr><td>CVSS 3.1 评级</td><td>高危</td><td>CVSS 3.1 分数</td><td>9.8</td></tr>
<tr><td rowspan="8">CVSS 向量</td><td colspan="2">访问途径（AV）</td><td>攻击复杂度（AC）</td></tr>
<tr><td colspan="2">网络</td><td>低</td></tr>
<tr><td colspan="2">用户认证（Au）</td><td>用户交互（UI）</td></tr>
<tr><td colspan="2">无</td><td>不需要</td></tr>
<tr><td colspan="2">影响范围（S）</td><td>机密性影响（C）</td></tr>
<tr><td colspan="2">不改变</td><td>高</td></tr>
<tr><td colspan="2">完整性影响（I）</td><td>可用性影响（A）</td></tr>
<tr><td colspan="2">高</td><td>高</td></tr>
<tr><td>利用条件</td><td colspan="3">无</td></tr>
<tr><td>危害描述</td><td colspan="3">未经身份认证的远程攻击者可以通过该漏洞在服务器上执行任意代码，从而获取服务器权限。</td></tr>
</table>

# 第四章 处置建议

目前官方已有可更新版本，建议受影响用户升级至最新版本：

GeoServer 2.23.* >= 2.23.6

GeoServer 2.24.* >= 2.24.4

GeoServer 2.25.* >= 2.25.2

同时，官方已发布先前版本的补丁可供下载，包括已修复的 gt-app-schema、gt-complex 和 gt-xsd-core jar 文件。

补丁可从以下 GeoServer 版本的发布页面下载：

2.25.1、2.24.3、2.24.2、2.23.2、2.21.5、2.20.7、2.20.4、2.19.2、2.18.0。

下载后使用补丁文件替换原文件即可。

您可以从此处获取官方补丁下载地址：

https://github.com/geoserver/geoserver/releases

**缓解措施：**

从 GeoServer 中删除“gt-complex-x.y.jar”文件，其中“xy”是 GeoTools 版本（例如，如果运行 GeoServer 2.25.1，则为“gt-complex-31.1.jar”）。这将从 GeoServer 中删除易受攻击的代码，尤其是需要 gt-complex 模块时，可能会破坏某些 GeoServer 功能或导致 GeoServer 部署失败。

# 第五章 产品解决方案

## 6.1 奇安信自动化渗透测试系统检测方案

奇安信自动化渗透测试系统已经能够有效检测针对该漏洞的攻击，请将插件版本和指纹版本升级到 202407052600 以上版本。规则名称：GeoServer CVE-2024-36401 远程代码执行漏洞。奇安信自动化渗透测试系统规则升级方法：系统管理->升级管理->插件升级（指纹升级），选择“网络升级”或“本地升级”。

## 6.2 奇安信开源卫士已支持

奇安信开源卫士 20240703. 677 版本已支持对 GeoServer 远程代码执行漏洞(CVE-2024-36401)的检测。

## 6.3 奇安信网神网络数据传感器系统产品检测方案

奇安信网神网络数据传感器（NDS5000/7000/9000 系列）产品，已具备该漏洞的检测能力。规则 ID 为：5754，建议用户尽快升级检测规则库至 2407031130 以上；

## 6.4 奇安信天眼产品解决方案

奇安信天眼新一代威胁感知系统在第一时间加入了该漏洞的检测规则，请将规则包升级到 3.0.0703.14394 及以上版本。

规则名称：GeoServer 远程代码执行漏洞(CVE-2024-36401)

规则 ID：0x10021C21

奇安信天眼流量探针（传感器）升级方法：系统配置->设备升级->规则升级，选择“网络升级”或“本地升级”。

## 6.5 奇安信网站应用安全云防护系统已更新防护特征库

奇安信网神网站应用安全云防护系统已全局更新所有云端防护节点的防护规则，支持对GeoServer 远程代码执行漏洞(CVE-2024-36401)的防护。

# 第六章 参考资料

[1]https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv

[2]https://github.com/geotools/geotools/pull/4797

[3]https://osgeo-org.atlassian.net/browse/GEOT-7587

# 奇安信 CERT

## 【我们是谁】

奇安信应急响应中心（奇安信 CERT）成立于 2016 年，隶属于奇安信旗下的威胁情报中心，旨在致力于向客户提供监测全面、响应迅速、认定客观、建议可行的漏洞情报。早在 Oracle 2020 年第二季度关键补丁更新公告中，就被评为了“在线状态安全性贡献者”。多次率先发现 WebLogic、Jackson 等知名软件和组件的高危漏洞并获得官方致谢。在风险通告方面，多次率先为客户提供漏洞和网络安全事件的风险通告、响应处置建议、相关技术分析和奇安信相关产品的解决方案。同时奇安信 CERT 在 Web 漏洞研究、二进制漏洞研究、前瞻性攻防工具预研等方面均积累了丰富的经验。

## 【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。

深度分析报告：深度分析报告是漏洞情报的一个增值服务，包含漏洞验证程序（PoC/EXP）、复现测试流量数据包、安全设备侧监测告警规则等额外的漏洞分析内容及防护措施。

## 【订阅方式】

安全风险通告（免费）：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

漏洞深度分析报告（付费）：扫描下方深度分析报告订阅服务预申请二维码留下联系方式，我们会与您联系并为您定制专属的漏洞情报服务。

**深度分析报告订阅服务预申请**

## 【微信公众号】

**奇安信 CERT**