安全漏洞通告

CVE-2020-36239：Jira 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2020-36239：Jira 远程代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-072302
报告版本	1	报告日期	2021-07-23
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-07-23	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 23 日，360CERT 监测发现 Atlassian官方 发布了 Jira远程代码执行 的风险通告，漏洞编号为 CVE-2020-36239 ，漏洞等级：严重，漏洞评分：9.8。

JiraSoftware 是一款强大的工作管理工具，从需求和测试用例管理到敏捷软件开发，它适用于各种类型的用例。该漏洞是由于Jira的开源组件Ehcache的RMI缺少认证，攻击者能够构造特定请求造成远程代码执行。

对此，360CERT 建议广大用户及时将 Jira 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
攻击者价值	高
利用难度	低
360CERT 评分	9.8

3 漏洞详情

3.1 CVE-2020-36239: Jira 代码执行漏洞

CVE: CVE-2020-36239

组件: Jira Data Center, Jira Core Data Center, Jira Software Data Center,Jira Service Management Data Center

漏洞类型: 代码执行

影响: 服务器接管

简述: 该漏洞影响JiraDataCenter和JiraServiceManagementDataCenter，其中JiraDataCenter包括JiraSoftwareDataCenter和JiraCoreDataCenter。以上产品的开源组件Ehcache的RMI服务缺少认证，并且默认情况下暴露在 40001 端口，远程攻击者可以在不需要任何身份验证的情况下连接到该端口，并在 JIRA 中通过反序列化任意对象造成代码执行。

4 影响版本

组件	影响版本	安全版本
Jira Data Center, Jira Core Data Center, Jira Software Data Center	>= 6.3.0 / < 8.5.16	8.5.16
Jira Data Center, Jira Core Data Center, Jira Software Data Center	>= 8.6.0 / < 8.13.8	8.13.8
Jira Data Center, Jira Core Data Center, Jira Software Data Center	>=8.14.0 / < 8.17.0	8.17.0
Jira Service Management Data Center	>= 2.0.2 / < 4.5.16	4.5.16
Jira Service Management Data Center	>= 4.6.0 / < 4.13.8	4.13.8
Jira Service Management Data Center	>= 4.14.0 / < 4.17.0	4.17.0

5 修复建议

5.1 通用修补建议

根据影响版本中的信息，排查并升级到安全版本。产品对应的下载地址为：

Jira Core Server: https://www.atlassian.com/software/jira/core/download

Jira Software Data Center: https://www.atlassian.com/software/jira/update

Jira Service Management Data Center: https://www.atlassian.com/software/jira/service-management/update

5.2 临时修补建议

通过防火墙等类似技术限制对JiraDataCenter, JiraCoreDataCenter, JiraSoftwareDataCenter, JiraServiceManagementDataCenter 的 EhcacheRMI 端口的访问。

6 时间线

2021-07-21 Atlassian 官方发布通告

2021-07-23 360CERT 发布通告

7 参考链接

Jira Data Center And Jira Service Management Data Center Security Advisory 2021-07-21

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn) 获取对应产品。

A.2 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元(探针）规则和本地安全大脑关联分析规则，做好防护。

A.3 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。