安全漏洞通告

【通告更新】CVE-2021-26084：Confluence OGNL 注入漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	【通告更新】CVE-2021-26084：Confluence OGNL 注入漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-090101
报告版本	2	报告日期	2021-08-26
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
2	2021-08-26	360CERT	360CERT	更新报告

目录

1 漏洞简述

2021 年 08 月 26 日，360CERT 监测发现 Atlassian官方 发布了 ConfluenceOGNL注入漏洞 的风险通告，漏洞编号为 CVE-2021-26084 ，漏洞等级：高危，漏洞评分：8.8。目前该漏洞安全补丁已更新，漏洞细节已公开，POC（概念验证代码）已公开，在野利用未发现。

该漏洞的 POC 与漏洞细节在网上已经公开。

对此，360CERT 建议广大用户及时将 Confluence 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 相关组件

Confluence是Atlassian公司的一个专业的企业知识管理与协同软件，也可以用于构建企业 wiki，因此，Confluence的使用面很广。在某些情况下，未授权的攻击者可以构造特殊的请求，造成远程代码执行。

Confluence Cloud 不受该漏洞影响

3 漏洞状态

类别	状态
安全补丁	已公开
漏洞细节	已公开
poc	已公开
在野利用	未发现
相关安全事件	未发现

4 风险等级

评定方式	等级
威胁等级	高危
影响面	广泛
攻击者价值	高
利用难度	低
360CERT 评分	8.8

5 漏洞详情

5.1 CVE-2021-26084: Confluence OGNL 注入漏洞

CVE: CVE-2021-26084

组件: Confluence Server & Confluence Data Center

漏洞类型: 代码执行

影响: 服务器接管

简述: ConfluenceServer 和 ConfluenceDataCenter 上存在一个 OGNL 注入漏洞，允许经过身份验证或在某些情况下未授权的攻击者，在 ConfluenceServer 或 ConfluenceDataCenter 实例上执行任意代码。

相关事件：暂无

6 影响版本

组件	影响版本	安全版本
Confluence Server & Confluence Data Center	< 6.13.23	6.13.23
Confluence Server & Confluence Data Center	< 7.11.6	7.11.6
Confluence Server & Confluence Data Center	< 7.12.5	7.12.5
Confluence Server & Confluence Data Center	< 7.4.11	7.4.11
Confluence Server & Confluence Data Center	-	7.13.0

7 修复建议

7.1 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，官方下载链接为：
https://www.atlassian.com/software/confluence/download-archives

7.2 临时修补建议

如果无法立即升级 Confluence，请参考官方通告 Mitigation（缓解） 一栏里针对 Linux/Windows 下用户给出的临时建议：
Atlassian 官方通告

8 时间线

2021-08-25 Atlassian 官方发布通告

2021-08-26 360CERT 发布通告

9 参考链接

Atlassian 官方通告

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。