关于Confluence OGNL 注入漏洞风险提示（CVE-2021-26084）

漏洞相关 吴昊A 2021-08-30 发表

漏洞描述

Confluence是一个企业级的Wiki，可用于企业、部门、团队内部进行信息共享和协同编辑。此次漏洞存在于Confluence Server 和 Data Center中 (Atlassian Confluence Cloud不受影响)。攻击者在特定情况下可以通过构造恶意OGNL表达式，进而在服务器上执行任意代码，控制服务器。目前暂未发现公开的POC和在野利用。 1.2 漏洞编号 CVE-2021-26084 1.3 漏洞等级 高危 二、修复建议 2.1 受影响版本 Confluence Server 和 Data Center的下列版本中存在该漏洞： Verison 4.xx Verison 5.x x Verison 6.0.x、6.1.x 、6.2.x 、6.3.x 、6.4.x 、6.5.x 、6.6.x 、6.7.x 、6.8.x 、6.9.x 、6.10.x 、6 .11.x 、 6.12.x 、6.13.x < 6.13.23、6.14.x 、6.15.x Verison 7.1.x 、7.2.x 、7.3.x 、7.4.x < 7.4.1 1、7.5.x 、7.6.x 、7.7.x 、7.8.x 、7.9.x 、7.10.x、7.11.x < 7.11.6、7.12.x < 7.12.5 2.2 修复建议 目前官方已经发布了修复该漏洞的安全更新，建议受影响用户尽快升级到安全版本。 下载地址为： ht tps://www.atlassian.com/software/confluence/download-archives

漏洞解决方案

以上产品均不涉及