网络安全风险预警通报

2021 年第 2 期 （总第 14 期）

广西大学网络信息中心 2021 年 6 月 10 日

【预警类型】 高危预警

【预警内容】

用友 NC BeanShell
存在远程代码执行漏洞的安全公告

安全公告编号 CNTA-2021-0021

一、漏洞概述

用友 NC 采用 J2EE 架构，面向大型企业集团和成长中的集团企业的信息化需求，为集团企业提供建模、开发、集成、运行、管理一体化的信息化解决方案。用友 NCBeanShell 远程代码执行漏洞（CNVD-2021-30167）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞利用细节已公开，用友公司已发布版本补丁完成修复，建议用户尽快更新至最新版本。

二、漏洞详情

2021 年 6 月 2 日，用友公司发布了关于用友 NC BeanShell 远程代码执行漏洞的风险通告。由于用友 NC 对外开放了 BeanShell 的测试接口，未经身份验证的攻击者利用该测试接口,通过向目标服务器发送恶意构造的 Http 请求，在目标系统上直接执行任意代码，从而获得目标服务器权限。

三、漏洞影响范围

漏洞影响的产品版本包括：用友 NC 6.5

四、漏洞处置建议

目前，用友公司已发布补丁完成漏洞修复，并通过服务渠道推送解决方案，授权用户可以通过访问链接进行下载。该漏洞对部署于公共互联网上的用友 NC 6.5 系统构成一定的安全风险，建议产品用户立即通过官方网站安装最新补丁，及时消除漏洞隐患：

http://umc.yonyou.com/ump/querypatchdetailedmng?PK=18981c7af483007db179a236016f594d37c01f22aa5f5d19