

知 关于iNode管理中心iNodeMngChecker.exe进程存在缓冲区溢出漏洞问题的公告.doc

iNode 李瑞峰 2013-05-03 发表

关于iNode管理中心iNodeMngChecker.exe进程存在缓冲区溢出漏洞问题的公告

【产品型号】

iNode 管理中心

【涉及版本】

5.2 C0407及之前的iNode管理中心版本。

【问题描述】

管理员安装运行iNode管理中心后iNodeMngChecker.exe进程存在缓冲区溢出漏洞，攻击者可以远程发送TCP攻击数据包，触发漏洞溢出，执行攻击shell。

【原因分析】

iNode管理中心进程iNodeMngChecker.exe启动时会绑定TCP 9090端口接收报文，解析报文中的属性时没有对属性的长度进行校验，当属性长度超长时会导致缓冲区溢出，造成攻击。

【解决方案】

iNode后续版本在从接收的报文中解析属性放到缓存中时增加对报文长度的校验，从而解决该问题。解决问题的版本合入iNode PC 5.2（C0408）及后续iNode版本，将在2013年5月8日发布。