河南省教育信息安全监测中心

木云电子科技资源统一管理平台敏感文件读取漏洞预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2023 年 07 月 04 日

木云电子科技资源统一管理平台敏感文件读取漏洞预警

事件描述

近期发现，木云电子科技资源统一管理平台存在一处文件读取漏洞，在处理文件读取的请求时，未对用户输入的参数进行验证，攻击者可以构造特殊的带有/../的请求，触发/etc/password、/etc/shadow 等敏感文件的读取。该漏洞威胁级别被定义为【中危】。

影响范围

木云电子科技资源统一管理平台

安全建议

1、核实本单位资产是否有木云电子科技资源统一管理平台。

2、若部署了木云电子科技资源统一管理平台，请联系厂商，参考如下建议对应用系统做升级：

1）输入过滤：需要对用户的输入进行严格的验证及过滤。

2）检查路径：在使用输入来构造路径之前，需要检查路径是否存在于预期的目录中。如果路径指向系统中未授权访问的目录，应该立即停止程序的执行，并返回错误。

3）使用绝对路径：为了避免路径穿越攻击，最好使用绝对路径而不是相对路径。相对路径可能会导致程序访问不想访问的目录。使用绝对路径可以确保程序只访问所期望的目录。

4）限制访问：为了保护系统中的文件和目录，应该限制程序的访问权限。程序只应该访问必要的文件和目录，不应该访问不需要的文件或目录。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052