防灾科技学院信息化管理中心

信息中心〔2021〕12 号

关于印发《防灾科技学院信息系统安全补丁更新管理规定》的通知

学校各部门、各单位：

为降低学校信息系统的安全隐患发生的可能性，明确补丁更新所涉及的步骤，使系统安全管理专员能够更好地对各种补丁进行更新操作，特制定《防灾科技学院信息系统安全补丁更新管理规定》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 10 月 7 日

防灾科技学院信息系统安全补丁更新管理规定

第一章　总则

第一条　为降低防灾科技学院（以下简称“学院”）信息系统的安全隐患发生的可能性，明确补丁更新所涉及的步骤，使系统安全管理专员能够更好地对各种补丁进行更新操作，并保证其有效性、稳定性和安全性，特制定本规定。

第二条　本规定的具体目标是：

（一）规范不同操作系统、应用程序、硬件设备系统的补丁定期检查。

（二）确认补丁安装的需求和申请的步骤。

（三）提供补丁更新流程在变更流程中所涉及的各项细化表格。

（四）规定各安全相关职员在补丁更新中的职责。

第三条　本规定适用于个人主机操作系统、生产主机系统、非生产主机系统、安全补丁管理。

第二章　职责分工

第四条　信息化管理中心：

（一）确认待安装补丁。

（二）通告服务器管理员执行补丁安装。

（三）统计终端与服务器补丁完成进度情况。

第五条　服务器管理员：

（一）管理和维护所辖范围服务器。

（二）监督和管理服务器的补丁分发、测试、安装和重启。

（三）执行服务器补丁的具体实施工作。

第六条 应用所属人：

负责及时反馈服务器补丁分发、测试、安装和重启过程中的应用运行状况。

第七条 补丁发布原因：

（一）修补应用程序或操作系统的漏洞。许多黑客通过缓冲区溢出对应用程序和操作系统进行网络攻击。通过补丁的安装能够对这类漏洞进行很好的修补。补丁也常常会由于修正系统的功能问题进行发布。

（二）改变功能或更新特征库等从而对新的安全威胁进行检测。

（三）修改软件的配置使它更加的安全。

第三章 补丁的登记和分类

第八条 安全补丁更新管理的目的是有效的审批和控制对于补丁的变更，从而减少对于业务和用户的影响，以达到较高的安全和实施性。

第九条 安全管理员发现规定范围内系统、应用程序或硬件有新补丁发布应向主管进行报告。同时主管在确认补丁后应责成相关安全负责人对补丁进行等级划分。

第四章 安全补丁风险与影响评估

第十条 根据不同的补丁等级，安全主管、安全运维人员与相关安装补丁系统的安全责任人组成评估小组对补丁的风险和影响进行定性评估，确定该补丁是否能够被加载。

第五章 补丁的审批

第十一条 补丁审批的输入主要是安全补丁风险与影响评估过程所生成的评估报告。经会议讨论后对补丁的安装与否进行判断。结果为驳回申请或授权补丁安装。

第十二条 对已授权安装的补丁应对补丁安装所需资源进行准备，同时通知相关责任人审批的结果。

第六章 安全补丁的开发测试与确认

第十三条 通过审批的补丁需由相应的负责人和相关应用系统部门主管进行开发测试。测试包括测试资源确认、测试方案设计、测试记录、测试结果输出、测试结果分析、测试改进以及最终接受补丁版本。

第七章 补丁的实施

第十四条 通过测试的补丁进行补丁实施流程。补丁的实施需由专员监督并由对应安全负责人进行安装。

第十五条 补丁的下载需要通过公司规定的安全途径，如系统软件文件服务器或从指定的系统供应商的官方网站上进行下载。

第十六条 补丁的安装时间由主管和相关应用服务部门经理进行确定。

第八章　补丁测试

第十七条　通过对的补丁实施后，对主机操作系统，应用服务进行测试，确认其可用性。

第九章　补丁回退

第十八条　若补丁实施不成功，则需要进行补丁回退流程。

第十九条　安全主管和相关应用服务部门经理需要授权补丁的回退工作并由相应的安全专员进行回退实施工作。

第二十条　回退成功后，安全主管需要对各相关部门进行通知，以确保所有相关人员都了解了补丁的回退工作并知晓其回退后可能带来的安全问题。

第十章　附则

第二十一条　本规定由信息化管理中心负责解释。

第二十二条　本规定自颁布之日起施行。

防灾科技学院信息化管理中心　　2021 年 10 月 7 日印发