“军队院校网络教学应用系统”漏洞的补救措施

□ 装甲兵工程学院教育技术中心 吴立元

内容摘要：本文针对“军队院校网络教学应用系统”的第一个版本集成管理工具的bug，给出了一个服务器端的部分补救的办法。

“军队院校网络教学应用系统”第一个版本的客户端集成管理工具存在一个漏洞，会泄露服务器的配置、FTP上传帐号/密码等信息，这严重影响系统的安全。虽然在后来的版本中这一错误已经修正，但是如果用户继续使用旧版本客户端集成管理工具的话，仍然可以得到服务器的配置，FTP上传帐号/密码等信息的，所以服务器端也应该有相应的补救措施的。

一、服务器配置信息的补救措施

所有服务器配置信息都保存在serverinf表中，由于服务器的配置信息不是经常改变的，所以可以把theguest对serverinf表的权限由“默认”该为“只读”，这样客户端就无法更改服务器的配置信息了。当需要修改配置信息时可以把表的权限改回，等配置修改完成再把表的权限恢复只读。或者直接修改表的内容就可以了。

操作步骤：mta数据库/serverinf表/属性/权限，对于theguest帐号只有select权限，禁止insert、update、delete权限。

二、FTP的补救措施

服务器端的FTP服务改用server-u来提供，对上传用户给予read、write、append、delete、create、remove权限。这样，即使用户得到FTP的用户名和密码，但登陆后由于没有list权限，仍然看不到任何东西，所以也就不会对服务器造成太大的威胁了。

假设原服务器配置如下：

资源的物理目录：D:\sc

FTP虚拟目录：ftpsc

FTP上传用户名：mirs

操作步骤：

（一）、计算机管理/系统工具/本地用户和组/用户：删除mirs帐号；

（二）、管理工具/internet服务管理器：删除原ftp站点；

（三）、sc文件夹/属性/安全：给予everyone修改、读取及运行、列出文件夹目录、读取、写入权限；

（四）、安装Server-U，不允许匿名访问；

（五）、Server-U Administrator / local server / domain / server / users：右键，newuser，添加用户mirs，mirs的home directory可指向原ftp目录，即：c:\inetpub\ftproot；

（六）、Server-U Administrator / local server / domain / server / settings / general / virtual path mappings：点add，在physical path输入d:\sc，next，map physical path to输入%home%，next，maped path name输入ftpsc，finish。至次，为Server-U添加完虚拟目录ftpsc。

（七）、Server-U Administrator / local server / domain / server / users / mirs / dir access：点add，file path输入d:\sc，finish。设定对d:\sc的存取权限：

files：read、write、append、delete

directories：create、remove

sub-directories：inherit

这样Server-U的配制就完成了。

以上的操作步骤是以Server-U 4.0为例的说明，不同的版本可能有差异。

（100072）北京丰台杜家坎21号装甲兵工程学院教育技术中心

wly1975@sohu.com