SNA Center/统一数字底盘关于检测到远端X服务正在运行中漏洞的整改方法

SNA Center 统一数字底盘 田毓磊 2024-01-30 发表

漏洞相关信息

漏洞编号： 不涉及
漏洞名称： 检测到远端X服务正在运行中
产品型号及版本： 不涉及

漏洞描述

X11协议是一种基于客户端/服务器模型的协议。X Server监听在6000/TCP端口，接受客户端发来的各种命令请求，服务器执行完命令后将事件返回给客户端。 如果允许从任意IP连接X Server的话，攻击者可能登录X Server并记录使用同一X Server的其它X Client的所有击键操作，这将包括帐号、密码等敏感信息。

漏洞解决方案

整改步骤如下：

（1）在操作系统后台执行vi /etc/ssh/sshd_config命令，在sshd_config文件中将X11Forwarding参数由yes改为no；

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
```

（2）修改完成后执行:wq命令保存sshd_config文件修改结果，然后在后台执行service sshd restart命令。

```
[root@campus ~]# service sshd restart
Restarting sshd (via systemctl):                           [  OK  ]
[root@campus ~]#
```