关于美国 Netsarang 公司多款软件存在恶意代码情况的通报

近日，收到关于美国 Netsarang 公司多款软件存在恶意代码情况的报告。该公司的 Xshell、Xmanager 等远程链接产品使用的 nssock2.dll 模块中存在恶意代码，可导致用户服务器账号、密码等信息上传至特定服务器。目前，Netsarang 公司已针对上述受影响产品发布升级版本，用户可通过查看 nssock2.dll 模块的版本来确定是否受此安全问题影响，如受影响，请尽快将相关产品升级至最新版本。该事件的具体情况如下:

一、事件介绍

NetSarang 是美国的一家提供安全链接解决方案的公司，该公司的产品主要包括 Xmanager, Xmanager 3D, Xshell, Xftp 和 Xlpd 等远程链接软件。

Xmanager, Xshell, Xftp, Xlpd 等多款产品使用的 nssock2.dll 模块（5.0.0.26 版本）中存在恶意代码。攻击者可能通过该恶意代码获取用户服务器账号、密码、网络信息等信息，进一步实施远程攻击。截止目前，下列版本的产品确认存在恶意代码:

Xshell Build 5.0.1322

Xshell Build 5.0.1325

Xmanager Enterprise 5.0 Build 1232

Xmanager 5.0 Build 1045

Xmanager 5.0 Build 1048

Xftp 5.0 Build 1218

Xftp 5.0 Build 1221

Xlpd 5.0 Build 1220

二、危害影响

Xshell 、Xmanager、Xftp 等远程链接产品在安全运维中使用范围较广，如 Xshell 软件用于在 Windows 平台上安全访问 Unix/Linux 主机，Xmanager 用于在本地电脑同时运行 Unix/Linux 和 Windows 图形化程序。上述存在恶意代码的产品会通过 DNS 隧道发送数据，其中可能包含了用户服务器的账号、密码、IP 等信息，攻击者一旦获取以上信息，可进一步窃取或修改用户服务器的敏感信息，对用户服务器造成较为严重的影响。

三、自查方式

用户可通过查看 nssock2.dll 的版本来确定是否受此影响，即在软件安装目录下找到 nssock2.dll 文件，右键该文件查看属性，如果版本号为 5.0.0.26 则存在恶意代码。

受影响的用户，可升级至 NetSarang 官方针对各软件发布的最新版本以消除漏洞影响。

四、修复建议

目前，NetSarang 官方已针对上述受影响产品发布升级

版本以修复此安全问题。请受影响用户及时检查是否受影响。如确认受到影响，请尽快升级最新版本。软件下载链接:

https://www.netsarang.com/download/software.htm

1