预警编号：YJ-2017020

恒安嘉新

关于 Xshell 系列软件被植入后门

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 08 月 15 日

1 漏洞简介

近期，互联网爆出 NetSarang 公司旗下 Xmanager 和 Xshell 等多款产品存在后门漏洞。2017 年 8 月 7 日，NetSarang 发布公告称，2017 年 8 月 4 日与卡巴斯基工程师发现远程连接系列软件中存在后门，官方公告地址：https://www.netsarang.com/news/security_exploit_in_july_18_2017_build.html。

2 漏洞原理

Xshell 是一款强大、著名的终端模拟软件，被广泛地用于服务器运维和管理，Xshell 支持 SSH，SFTP，TELNET，RLOGIN 和 SERIAL 功能。

在 Xshell、Xlpd、Xmanager、Xftp 等安装目录下的相关的用于网络通信的组件 nssock2.dll 模块被发现存在后门类型的代码（样本 hash 值为：97363d50a279492fda14cbab53429e75），可能导致所敏感信息被泄露到攻击者所控制的机器。

受影响的 nssock2.dll 文件版本为 5.0.0.26，在 Xshell 5.0.1322 和 Xshell 5.0.1325 两个版本中均已确认恶意代码存在，DLL 本身有厂商合法的数据签名，调试发现发现其存在加载执行 Shellcode 的功能，Shellcode 会收集主机信息，生成一个月一个的 DGA 域名并尝试解析，并对 DGA 域名发起请求：

```
void *__thiscall sub_1000C6C0(void *this)
{
  void *v2; // [sp+0h] [bp-18h]@1
  int (__stdcall *v3)(_DWORD); // [sp+8h] [bp-10h]@1
  unsigned int i; // [sp+10h] [bp-8h]@1
  unsigned int v5; // [sp+14h] [bp-4h]@1

  v2 = this;
  v3 = (int (__stdcall *)(_DWORD))VirtualAlloc(0, 0xFB48u, 0x1000u, 0x40u);
  v5 = encrypted_shellcode;
  for ( i = 0; i < 0xFB44; ++i )
  {
    *((_BYTE *)v3 + i) = v5 ^ *((_BYTE *)&encrypted_shellcode + i + 4);
    v5 = 0xC9BED351 * ((v5 >> 16) + (v5 << 16)) - 0x57A25E37;
  }
  if ( (unsigned int)v3(0) < 0x1000 )
    MessageBoxA(0, "###ERROR###", 0, 0);
  return v2;
}
```

图一 对 DGA 域名发起请求

其中一个域名为“nylalobghyhirgh.com”，该域名开启了隐私保护

域名 nylalobghyhirgh.com 的信息 以下信息更新时间：2017-08-14 16:40:00 立即更新

域名	nylalobghyhirgh.com [whois 反查] 其他常用域名后缀查询： cn com cc net org
注册商	NameSilo, LLC
联系人	domain administrator [whois反查]
联系邮箱	pw-04e02d999b02a1ff9d29d1f03386464d@privacyguardian.org [whois反查]
联系电话	13478717726 [whois反查]
创建时间	2017年07月23日
过期时间	2018年07月23日
公司	See PrivacyGuardian.org
域名服务器	whois.namesilo.com
DNS	NS1.QHOSTER.NET NS2.QHOSTER.NET NS3.QHOSTER.NET NS4.QHOSTER.NET

图二 nylalobghyhirgh.com 信息

2017 年整个 DGA 域名为：

1 月域名:tgpupqtylejgb.com

2 月域名:psdghsbujex.com

3 月域名:lenszqjmdilgdoz.com

4 月域名:huxerorebmzir.com

5 月域名:dghqjqzavqn.com

6 月域名:vwrcbohspufip.com

7 月域名:ribotqtonut.com

8 月域名:nylalobghyhirgh.com

9 月域名:jkvmdmjyfcvkf.com

10 月域名:bafyvoruzgjitwr.com

11 月域名:xmponmzmxkxkh.com

12 月域名:tczafklirkl.com

对 12 个域名分析 NS 解析情况后发现，从 7 月开始才被注册解析到 qhoster.net 的 NS Server 上 ,所以我们猜测这个恶意代码事件至少是从 7 月开始的。

3 影响范围

受影响的 nssock2 版本：

nssock2.dll: 5.0.0.26

MD5：97363d50a279492fda14cbab53429e75

SHA-1:f1a181d29b38dfe60d8ea487e8ed0ef30f064763

受影响的产品如下：

Xmanager Enterprise 5.0 Build 1232

Xmanager 5.0 Build 1045

Xshell 5.0 Build 1322

Xftp 5.0 Build 1218

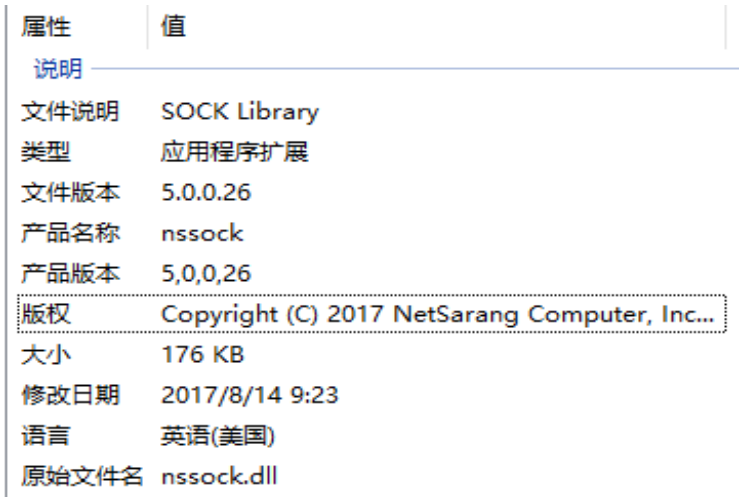
Xlpd 5.0 Build 1220

4 修复建议

用户可通过查看 nssock2.dll 的版本来确定是否受此影响：

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 则存在后门代码：

图三 签名列表



图四 查看属性

NetSarang 已于 8 月 5 日更新了各软件版本，请及时升级。最新版本如下：

Xmanager Enterprise Build 1236

Xmanager Build 1049

Xshell Build 1326

Xftp Build 1222

Xlpd Build 1224

最新 Builds 下载地址:

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