



某制造业集团 NetScout 平台漏洞修复方案

北京一实天勤科技有限公司

2022. 1

一、文档目的

针对 1 月份漏洞，特编写此文档，对 NetScout 底层进行补丁修复，以保障企业安全。

二、修补时长及影响

1. 预计整体修补在 1 个小时内完成。
2. 修补完成后需对设备进行重启，重启期间，发送过来的流量无法记录。
3. 设备旁路部署，重启期间对网络无任何影响，远程操作即可。

三、详细步骤:

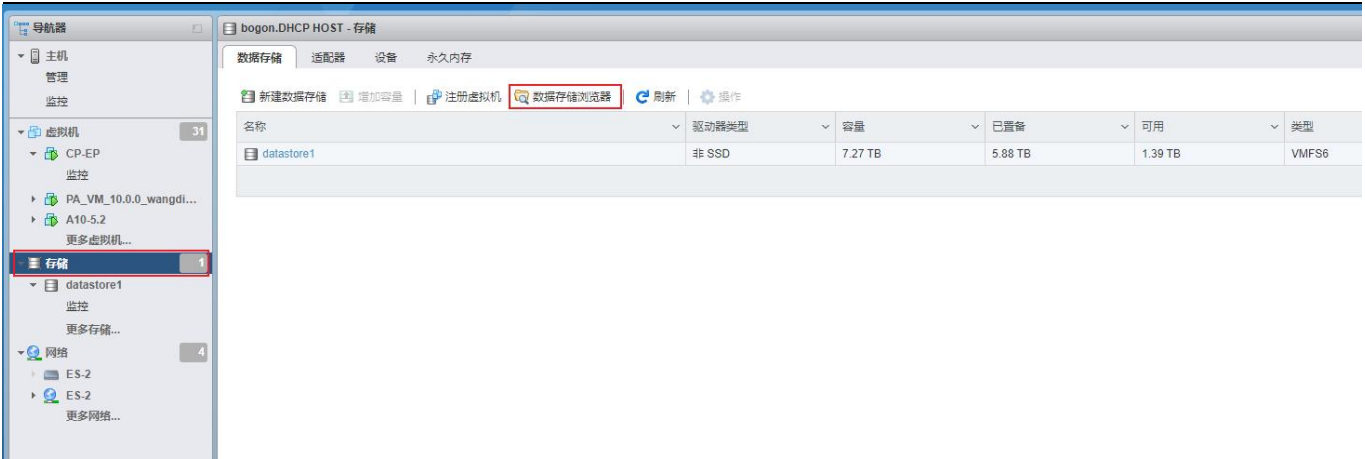
3.1 针对 plugin 名为 118466 118885 123518 143221 的漏洞。

1. 请下载补丁包链接如下:

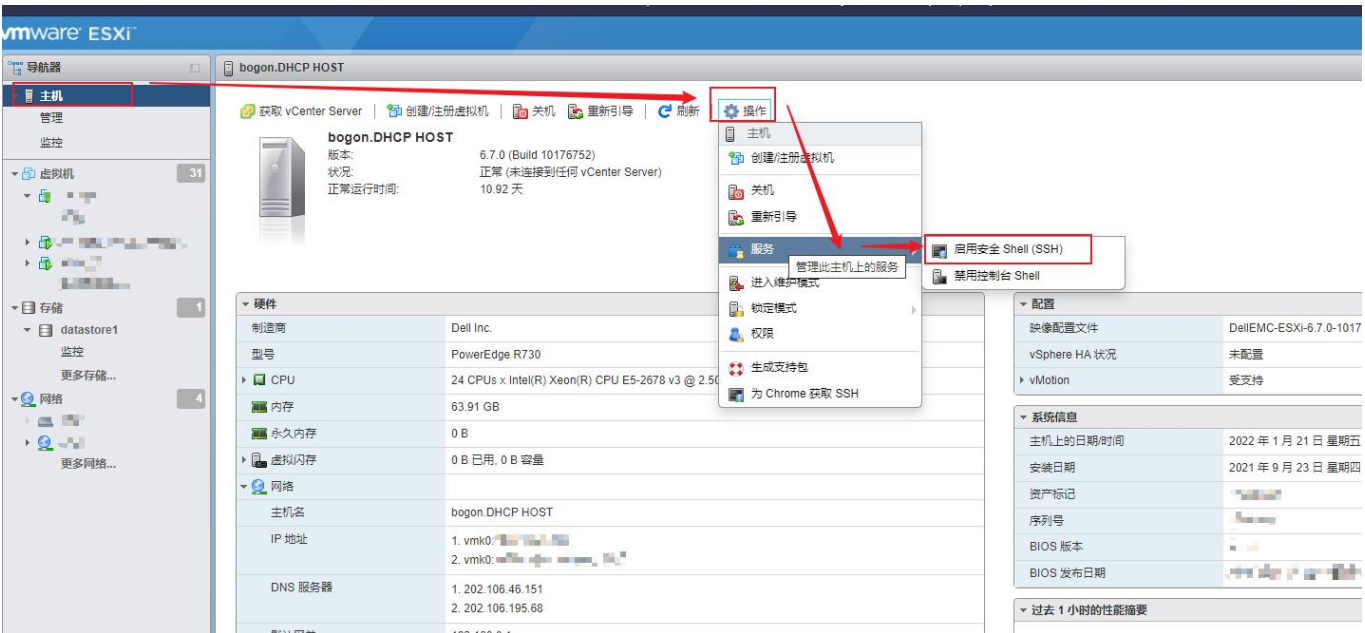
链接: <https://pan.baidu.com/s/1Y22w5D5bCCMMxib7aAzoyg>

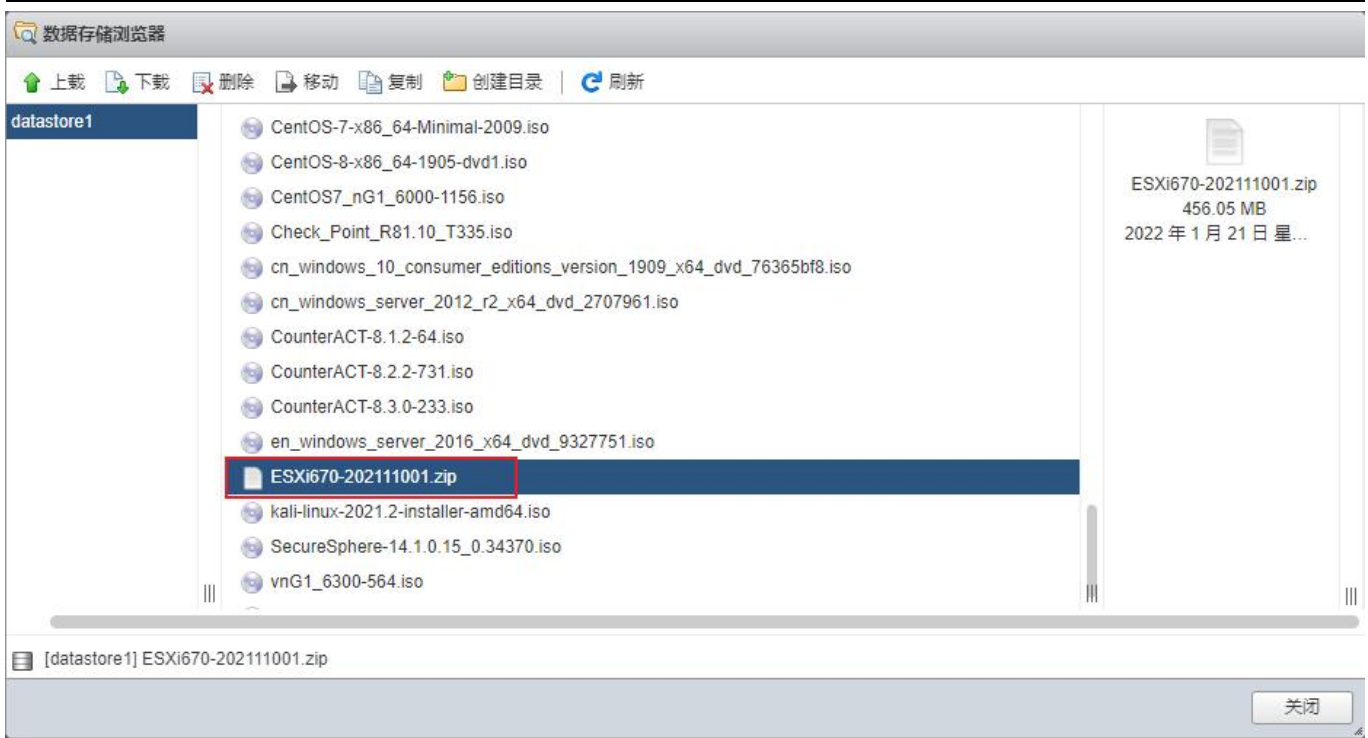
提取码: r9nh

2. 访问 [https:// 10.120.141.230/ui/#/login](https://10.120.141.230/ui/#/login)
3. 关闭运行虚拟机，点击数据存储浏览器，上传补丁包。

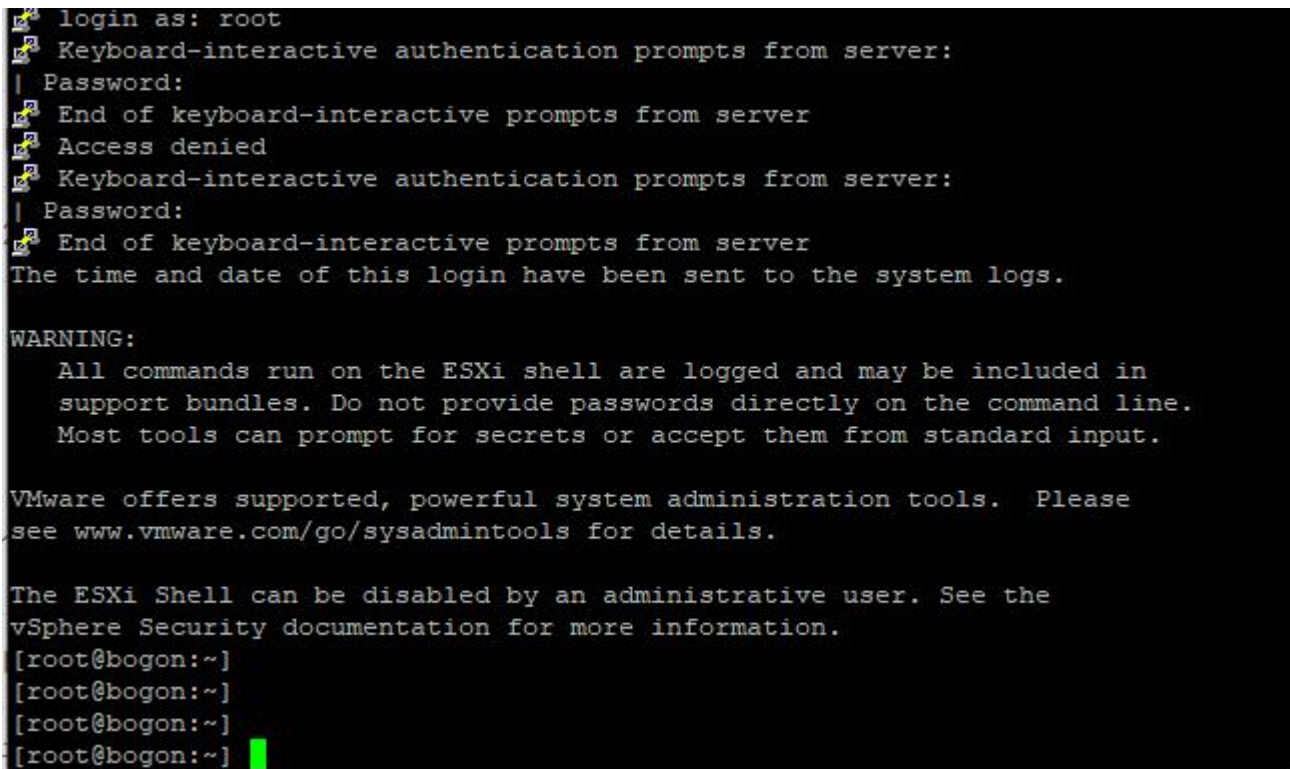


4. 主机界面打开 SSH 访问权限，并进入维护模式。





5. SSH 输入账号密码登录



6. 根据文件上传路径切换到补丁文件上传路径下

```
[root@bogon:/vmfs/volumes/607579cd-84f69b52-5cbd-246e96622d70] pwd
/vmfs/volumes/datastore1
[root@bogon:/vmfs/volumes/607579cd-84f69b52-5cbd-246e96622d70]
```

7. 安装补丁文件

```
esxcli software vib install
```

```
-d=/vmfs/volumes/6033a89a-9b302dcc-6ed2-0050569ee88e/ESXi670-202111001.
```

```
zip
```

注：该路径以实际路径为准。

```
[root@bogon:/vmfs/volumes/607579cd-84f69b52-5cbd-246e96622d70/patch] esxcli software vib install -d "/vmfs/volumes/datastore1/patch/ESXi670-202111001.zip"
Error: Unknown command or namespace software vib install

[root@bogon:/vmfs/volumes/607579cd-84f69b52-5cbd-246e96622d70/patch] esxcli software vib install -d "/vmfs/volumes/datastore1/patch/ESXi670-202111001.zip"
[DependencyError]
VIB QLC_bootbank_qedf_1.2.24.6-10EM.600.0.0.2768847 requires qedentv_ver = X.0.7.5, but the requirement cannot be satisfied within the ImageProfile.
VIB QLC_bootbank_qedrntv_3.7.9.2-10EM.670.0.0.7535516 requires qedentv_ver = X.0.7.5, but the requirement cannot be satisfied within the ImageProfile.
VIB QLC_bootbank_scsi-qedil_1.0.22.0-10EM.600.0.0.2494585 requires qedentv_ver = X.0.7.5, but the requirement cannot be satisfied within the ImageProfile.
Please refer to the log file for more details.
```

8. 升级结束后重启，查看补丁是否升级完成。



3.2 针对 plugin 名为 41028 的漏洞。

1. 可修改管理平台与设备探针之间的 SNMP 团体字，默认为 public。

2. ssh 进入设备探针底层系统，IP 为：10.120.141.245-247：

输入：isbin

```
./localconsole
```

选择 5/6 选项后更改团体字例如：neusoft，更改后如下图，团体字为 neusoft。

```
** Infinistream Model vSTREAM - CDM 6.3.2 (Build 489) **

Interface number : 3

Probe IP V4 address      192.168.0.120

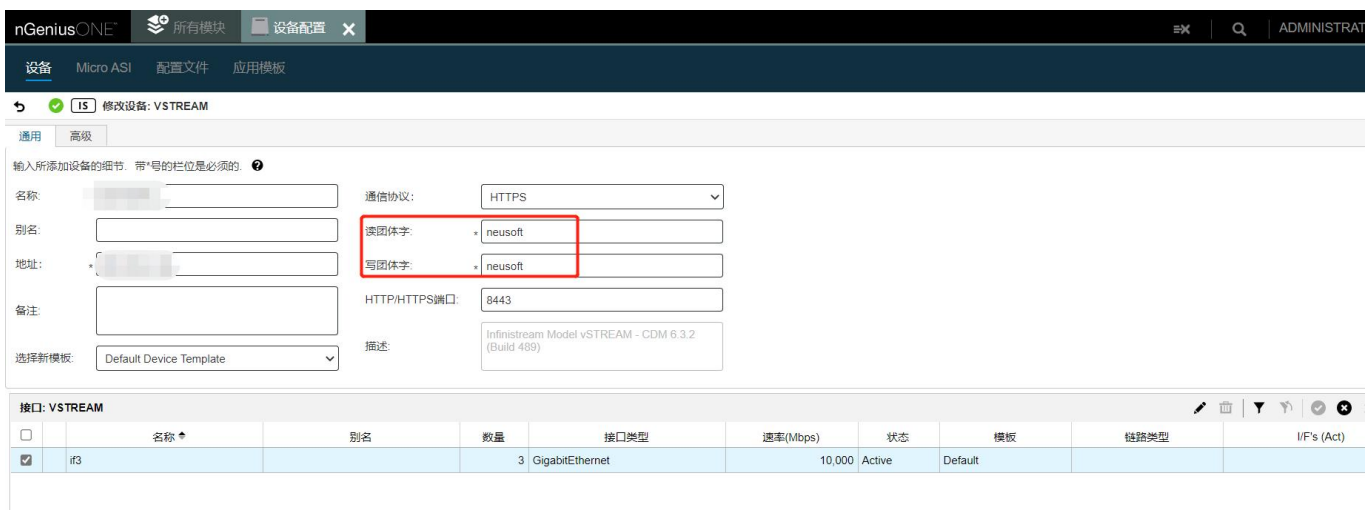
[4]  Change Config Server Address      192.168.0.128
[5]  Change Read Community             neusoft
[6]  Change Write Community            neusoft
[7]  Select Interface                  10 GIGABIT-ETHERNET
[8]  Software Options
[9]  Agent Options
[11] Enter Command-line mode
[12] Reset Agent
[13] Security Options
[14] Console Logout
[15] Protocol Options
```

3. 重启进程:

./stopall

./start

4. 在管理平台设备管理处修改团体字即可, 如下图:



The screenshot shows the 'nGeniusONE' management platform interface. The main window is titled '修改设备: VSTREAM'. The '通用' (General) tab is active. The configuration form includes fields for '名称' (Name), '别名' (Alias), '地址' (Address), '备注' (Remarks), and '选择新模板' (Select New Template). The '通信协议' (Communication Protocol) is set to 'HTTPS'. The '读团体字' (Read Community) and '写团体字' (Write Community) fields are both set to 'neusoft' and are highlighted with a red box. The 'HTTP/HTTPS端口' (HTTP/HTTPS Port) is set to '8443'. The '描述' (Description) field contains 'Infinistream Model vSTREAM - CDM 6.3.2 (Build 489)'. Below the form is a table titled '接口: VSTREAM' (Interface: VSTREAM) with the following data:

名称	别名	数量	接口类型	速率(Mbps)	状态	模板	链路类型	IF's (Act)
if3		3	GigabitEthernet	10,000	Active	Default		