

Sri Lanka Institute of Information Technology

**Linux Exploitation ( CVE-2014-0038 )**

**Individual Assignment**

IE2012 – Systems and Network Programming

Submitted by:

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT19115276 | Kiruthikan.S |

Date of submission

12/05/2020

**Introduction**

This assignment attempts to exploit CVE-2014-0038, by sending a recvmmsg system call with a crafted timeout pointer parameter to gain root. This exploit has offsets for 3 Ubuntu 13 kernels: 3.8.0-19-generic (13.04 default); 3.11.0-12-generic (13.10 default); 3.11.0-15-generic (13.10). I chose Ubuntu 13.10 for this assignment. This exploit may take up to 13 minutes to run due to a decrementing (1/sec) pointer which starts at 0xff\*3 (765 seconds). GR security and Pax found this vulnerability on 28th January 2014.

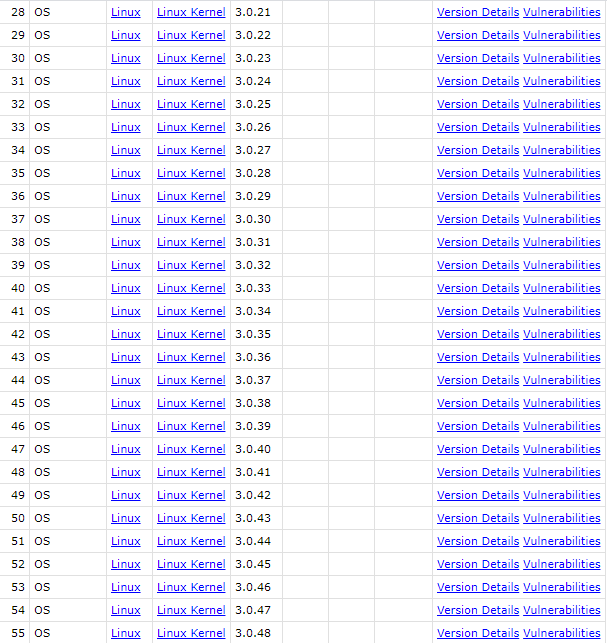
Vulnerability details,

A screenshot of a social media post

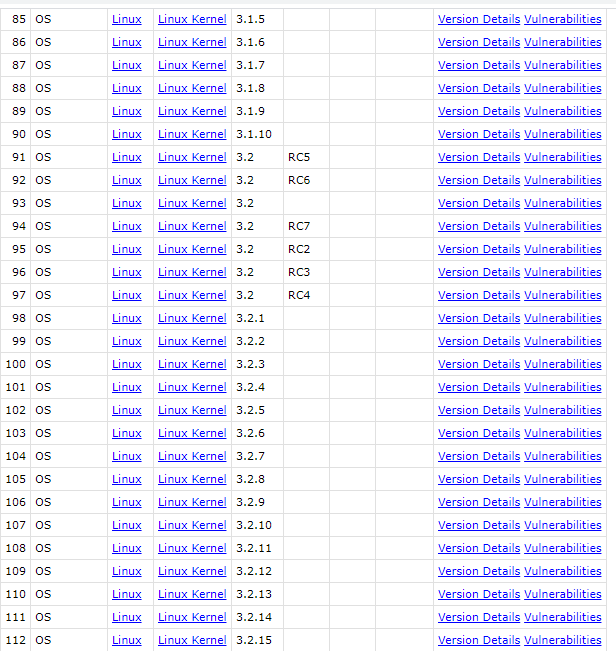
Description automatically generated

Products affected by CVE-2014-0038,

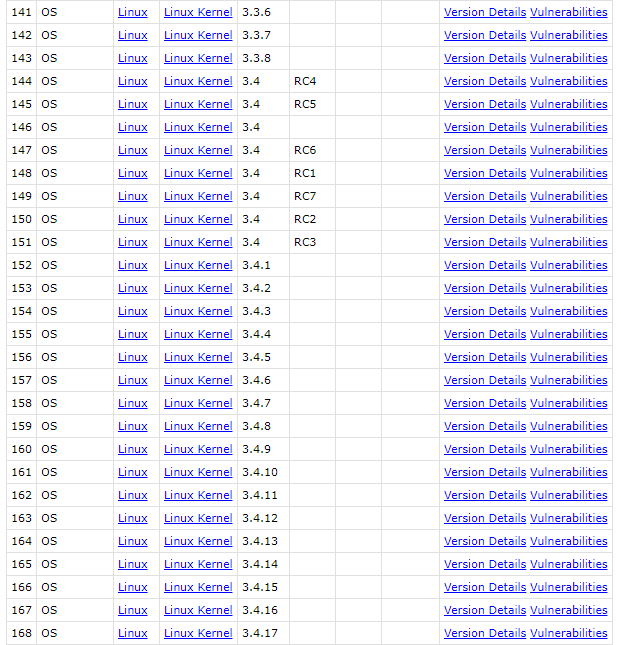






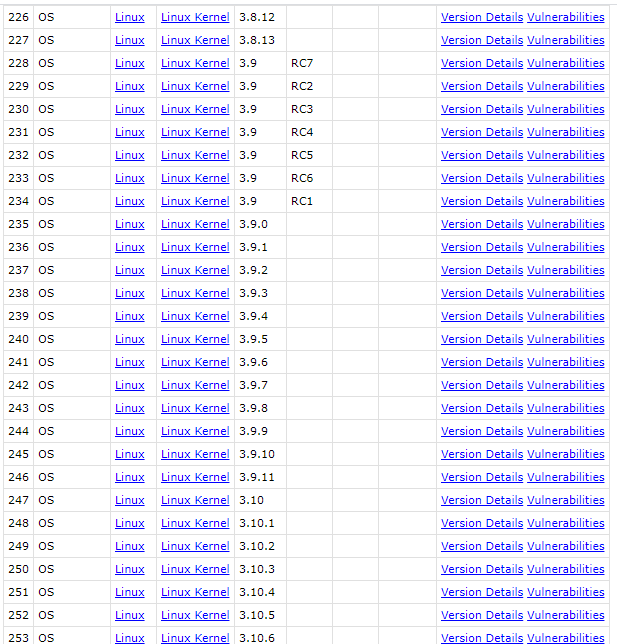




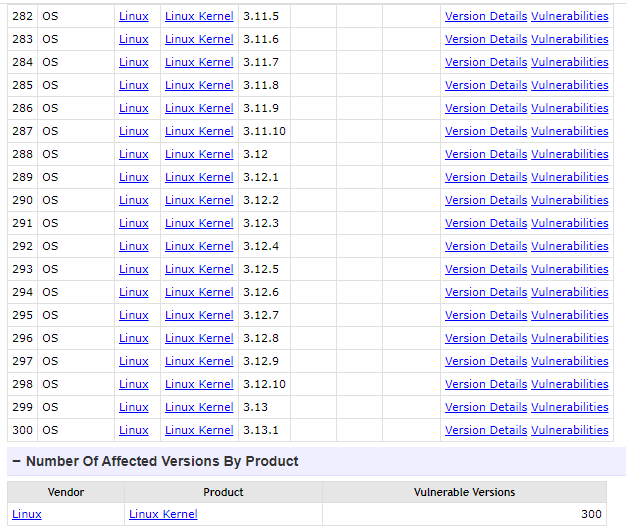












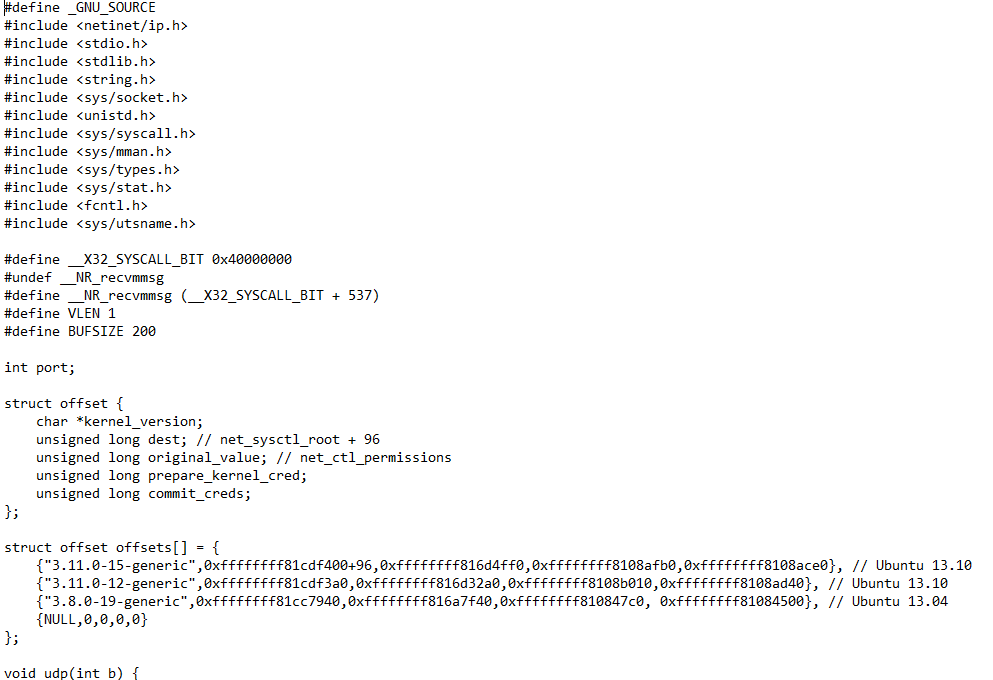
**Exploit**

There are three exploiting methods.

* Recvmmsg.c – Linux 3.4 + local root (CONFIG\_X86\_X32 = y)

CVE-2014-0038 / X32 ABI with recvmmsg

Author: rebel@irc.smashthestack.org

Coding of recvmmsg.c file is attached here,

A screenshot of a social media post

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

* Pass a pointer to a kernel address as timeout for recvmmsg,

1. If the original byte at that address is known, it can be overwritten.
2. If the least significant byte is 0xff , waiting 255 seconds will turn it into a 0x00.

Author: Saelo

Coding of this c file is attached here,



A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

Description automatically generated

A screenshot of a cell phone

Description automatically generated

* Linux kernel recvmmsg privilege escalation – Metasploit module.

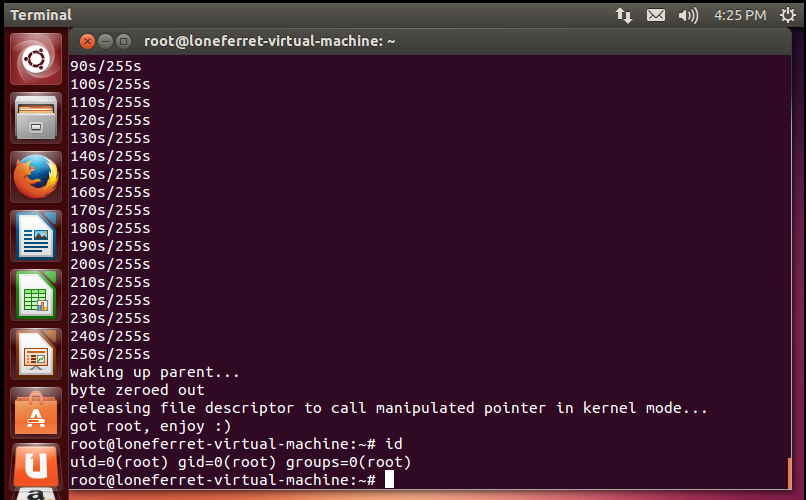
Author: Rebel and h00die <mike@shorebreaksecurity.com>

Commands of the Metasploit module is attached here,

A screenshot of a social media post

Description automatically generated

* Finally, I chose the second method and I have attached the output here,

****

**Conclusion**

This reported bug in the linux kernel’s recvmsg syscall when called from code using the x32 ABI. An unprivileged local user could exploit this flaw to cause a denial of service (system crash) or gain administrator privileges. This vulnerability can be corrected by updating your system to the following package versions,

Ubuntu 12.04 LTS

[linux-image-3.11.0-15-generic](https://launchpad.net/ubuntu/+source/linux-lts-saucy?_ga=2.47098863.93247232.1589285549-1080338157.1589285549) - [3.11.0-15.25~precise1](https://launchpad.net/ubuntu/+source/linux-lts-saucy/3.11.0-15.25~precise1)

[linux-image-3.11.0-15-generic-lpae](https://launchpad.net/ubuntu/+source/linux-lts-saucy) - [3.11.0-15.25~precise1](https://launchpad.net/ubuntu/+source/linux-lts-saucy/3.11.0-15.25~precise1)

**References**

1. <https://www.cvedetails.com/cve/CVE-2014-0038/>
2. <https://www.exploit-db.com/exploits/40503/>
3. <https://github.com/saelo/cve-2014-0038>
4. <https://code.google.com/p/chromium/issues/detail?id=338594>
5. <https://www.ubuntu.com/usn/USN-2096-1>
6. <https://bugzilla.redhat.com/show_bug.cgi?id=1060023>
7. <https://pastebin.com/raw.php?i=DH3Lbg54>
8. <https://secunia.com/advisories/56669>
9. <https://www.exploit-db.com/exploits/31346>
10. <https://www.exploit-db.com/exploits/31347>
11. <http://www.mandriva.com/security/advisories?name=MDVSA-2014:038>
12. <https://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=2def2ef2ae5f3990aabdbe8a755911902707d268>
13. <https://www.ubuntu.com/usn/USN-2094-1>
14. <https://www.openwall.com/lists/oss-security/2014/01/31/2>
15. <https://www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.13.2>
16. <http://lists.opensuse.org/opensuse-security-announce/2014-02/msg00003.html>
17. <http://lists.opensuse.org/opensuse-security-announce/2014-02/msg00002.html>
18. <https://www.ubuntu.com/usn/USN-2095-1>
19. <http://www.securityfocus.com/bid/65255>
20. <https://www.rapid7.com/db/modules/exploit/linux/local/recvmmsg_priv_esc>
21. <https://vimeo.com/88291815>