

Sri Lanka Institute of Information Technology

**Individual Assignment**

IE 2032 SOS

Submitted by:

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT19404042 | Soysa W.R.I |

Date of submission

12.05.2020

APT - Repository Signing Bypass via Memory Allocation Failure

**(CVE:**[2016-1252](https://nvd.nist.gov/vuln/detail/CVE-2016-1252))

****

**Introduction** **-Memory Allocation Failure**

This is about a exploitation through a memory allocation failure.Also these types of vulnerabilitys are hard to find.this vulnerability is found in 2016 december by google research team.Also this google team job is searching vulnerabilities in most using softwares, os platforms including google. When the research team found bug they reports to the company to fix the bug within 90 days.if they couldn’t fix the bug automatically google team will release the information about the bug and provides the general public with sample attack code .When apt get updates a repository that uses an InRelease file. [1] [2]

There are many ways to exploit a vulnerability.

* Penetration testing
* Using exploit tools
* Following the victim
* Audit network assets

These are the main ways to exploit.

* **Penetration testing**

This is using by the association to forestall the assaults.an assailant additionally can attempt this strategy to misuse.the assailant is continue attempting to assault the framework withproceeds with investigation of the framework works. Analyzer knowing all the frameworks and structures.for an aggressor it is difficult to get subtleties. Assailants adventure might be hurtful on the grounds that the analyzer didn’t figure the method of assault.

* **Using exploit tools**

This is most useful thing and attackers can handle this very easy way.most of the attackers using linux platforms because its open source framework.so the tools are metasploit , Nessus, burp suit and so forth once the casualty is chosen the device consequently check all the shortcoming of the casualty framework and the safety efforts of the objective framework. [3]

* **Following the victim**

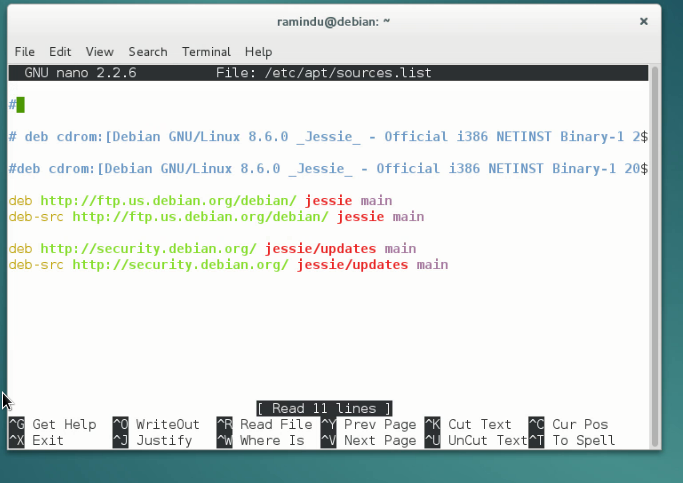
The assailant should gather the individual data and question the person theory the passwords or access pins utilizing the data.all the assailant need is a information in IQ and rationale. an aggressor needs to get the data of the casualty likewise the bio information.some people with familiarity with this sort of assaults.they keep their passwordsin an alternate way.but those are can get from guessing. [4]

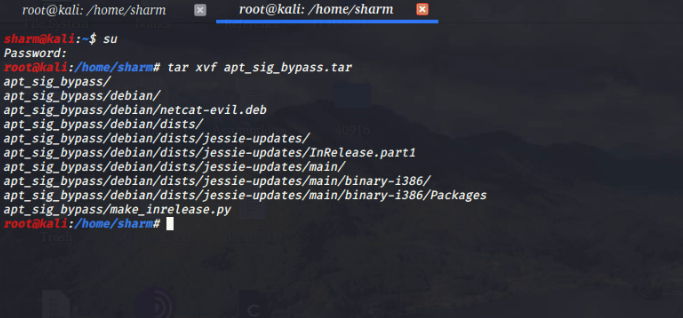
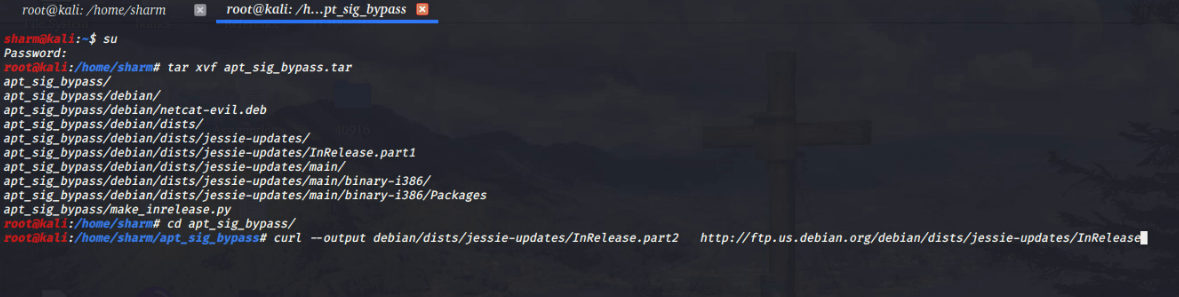
**Way to exploit**

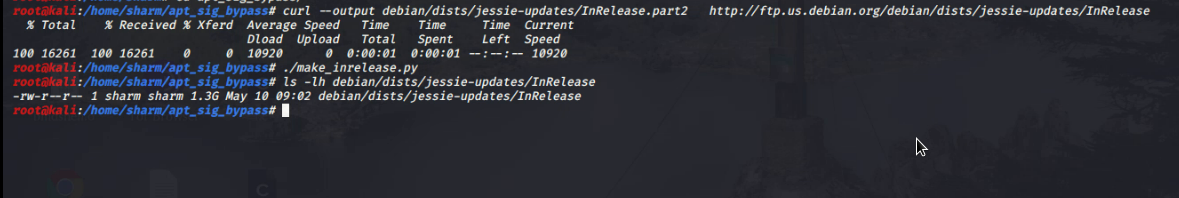
* **First code is to get the source list in debian**.

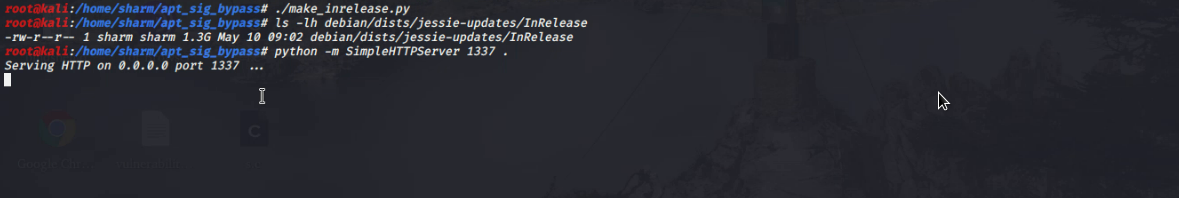


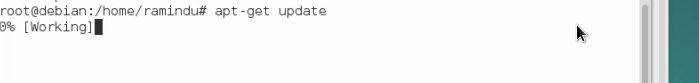
* **And this is the source list in debian machine.**



* **Then the attacker machine can unzip the tar file**.
* **After unzip the tar file attacker can get in to the file**.
* **After get in to the tar file attacker can download the malicious file to the attacker machine.**

****

* **After downloading the malicious file then attacker can get the SimpleHttpserver** 

**Then debian machine have to get the malicious file from the attacker machine. Then debian machine have to update . **

* **After the sucessfuly update the file then attacker have to verify that.so then**

**L:\SNP\debian2ndcode.png**

After this if attacker gets lucky with aslr randomaization,there are no security warnings and simply install the malicious version of the package.After this the malicious file attacking to the kernel then exploit it.

So this is the exploitation.

**Conclusion**

So for this exploitation needs the debian 8.6 version. In this attacker can create a inrelease file that is parsed as a proper split-signed file during signature validation. but isn’t recognized by the file.the leading garbage that was ignored by the signature validation is interpreted as repository metadata.

**Reference**

|  |  |
| --- | --- |
| [1] | "APT-Repository Signing Bypass via Memory Allocation Failure," [Online]. Available: https://www.exploit-db.com/exploits/40916. |
| [2] | "Common Vulnerability and Exposures," [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1252. |
| [3] | "ubuntu apk package," [Online]. Available: https://bugs.launchpad.net/ubuntu/+source/apt/+bug/1647467. |
| [4] | "how to create a sudo user on debian," [Online]. Available: https://linuxize.com/post/how-to-create-a-sudo-user-on-debian/. |
| [5] | [Online]. Available: https://www.exploit-db.com/exploits/40916. |
|  |  |
|  |  |
|  |  |
|  |  |

# 

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |