Tartu Ülikool
Loodus- ja Täppisteaduste Valdkond
Arvutiteaduse Instituut

CVE-2019-3462

Karel Paan

Õppezööd: Meelis Roos

Tartu 2019
Summary [1] [2]

CVE-2019-3462 is a vulnerability in the APT (Advanced Package Tool) [in Linux Ubuntu and Linux Debian], a high level package manager for requiring additional software to your PC. The vulnerability was in incorrect sanitation of the 302 redirect field in HTTP (Hypertext Transfer Protocol) transport method. This meant that it was possible to send altered packages to the host using the man-in-the-middle attack, making the host believe that no alterations were made. Also the content could later be used for executions with root privileges. The vulnerability was found by Max Justicz and was fixed after APT 1.4.8.

Linux Advanced Package Tool [3]

The crux of the matter is that Linux APT uses HTTP rather than the more secure HTTPS connection. And cryptographic signatures to check if the downloaded contents are same to the ones sent from the server. The signature itself is very similar to the Estonian Id card. Using HTTP meant that that the attacker using MITM attack could have injected a redirect into the HTTP headers to change the URL used to fetch the package. Furthermore the hacker would be able to manipulate the hashes used by the APT, passing legit values, to disguise the malware as sanctioned software from the original site.

The attack [3] [5]

A malicious person, that is using a MITM or any kind of package mirroring is able to execute unauthorized code as root on the victims computer, installing any package. This goes unnoticed by the host because we are able to insert are own redirect. This was abled due to the reason that the worker process returned a redirect instead of a URI Done after HTTP redirect. Thus the attacker is able to send to the host any kind of a hash, making it believe that the package hasn’t been tampered with. After falling for the attack we don’t just become victims of a data spoofing, we are bound to lose control over our entire computer. Because the package is installed with APT, it is by default allowed to use root commands, meaning they can add any kind of packages to our computer e.g. a Trojan Horse.
The fix [3] [4]

If we consider ourselves using 1.4.8 still, then to upgrade our system to the secure patch, we must first disable redirect, because for updating the APT, we must use APT itself, and as we know the packages could contain malware. This also serves as a fix for the problem itself due to the attack consists of redirecting our header, which is now impossible, thus our computer won’t be fooled by false certificates.

```
$ sudo apt update -o Acquire::http::AllowRedirect=false
$ sudo apt upgrade -o Acquire::http::AllowRedirect=false
```

Afterwards we should use

```
$ sudo apt-get update
```

Also there is a way to manually install the new version of APT wget or curl.

Should APT still use HTTP [3]

The founder of the bug, Max Justicz, himself believes that it is unnecessary until it uses cryptographic checks in the end. He also noted, that "I just think it’s worth making HTTPS repositories the default – the safer default – and allowing users to downgrade their security at a later time if they choose to do so." I believe that it is not a necessity because Linux, furthermore apt are tools for people who know what their doing, meaning they are not usually used for primal uses e.g. playing, watching videos. Therefore the users are aware of the dangers and are able to defend themselves against them. Although it makes the process of apt-get more convenient and secure, so it should be on the checklist for the Linux developers.
Used materials:


[3] https://www.theregister.co.uk/2019/01/22/debian_package_manager_flaws/
