Security Advisory-No: 37   **13, Feb 2019**

Threat Classification: Vulnerability

Name: Remote Code Execution Vulnerability **(CVE-2019-3462)**

Source: Affect following product of Linux OS:

- Advanced Package Tool (APT) 1.4.8 and older

Exploited Vulnerabilities:

An attacker could exploit this vulnerability through act himself as a man-in-the-middle between APT and mirroring to inject malicious content into HTTP connection. This content could be recognized as a valid package by APT and used later for code execution with root privileges on the target machine.

On Successful exploitation of this vulnerability, the attacker could fully compromise the victim machine and performs various malicious activities such as the unauthorized installation of any package, the creation of rogue administrator accounts and modification of user's data.

Recommendations:

a) Affected users and system administrators of Debian, Ubuntu, and other Linux distributions are advised to download and install the security updates immediately.

- https://lists.debian.org/debian-security-announce/2019/msg00010.html
- https://usn.ubuntu.com/3863-1/

b) In case of any incident, please report to this office.