AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Vulnérabilités critiques dans le gestionnaire de paquets APT

Contenu

I. Contexte

Debian a publié un avis de sécurité indiquant que leur gestionnaire de paquets était vulnérable à une injection de code.

Par défaut, les mises à jour sont récupérées en HTTP. Toutefois des vérifications sont effectuées en local afin d'assurer l'intégrité des fichiers récupérés. Un attaquant en position d'intercepteur actif (Man In The Middle) peut injecter un paquet malveillant qui sera considéré comme valide.

Cette vulnérabilité n'est présente que dans le cadre de l'utilisation de redirections par APT. Le logiciel APT s'exécute avec un niveau de privilège élevé, une attaque réussie garanti donc à l'attaquant une compromission totale du système. Il s'agit donc d'une vulnérabilité sérieuse, d'autant plus qu'elle impacte directement le mécanisme de mise à jour. Il est nécessaire d'appliquer le correctif tout en minimisant les risques d'exploitation.

II. Contournement provisoire

Uniquement dans le cadre de cette mise à jour, Debian recommande de désactiver les redirections par les commandes suivantes :

apt -o Acquire::http::AllowRedirect=false update;apt -o Acquire::http::AllowRedirect=false upgrade

Toutefois, cela peut ne pas fonctionner lorsque l'on est placé derrière un proxy et que l'on cherche à atteindre le miroir security.debian.org. Dans ce cas, il est possible d'utiliser la source suivante :

http://security-cdn.debian.org/debian-security/

Si la mise à jour d'APT sans la désactivation des redirections est impossible, il est alors recommandé de télécharger manuellement le paquet. Il convient ensuite d'effectuer la vérification d'intégrité avant de l'installer.

Référence CVE CVE-2019-3462

Systèmes affectés :

- APT versions antérieures à 1.4.9 sur Debian
- APT sans le dernier correctif de sécurité sur Ubuntu 12.04 ESM, 14.04 LTS, 16.04 LTS, 18.04 LTS et 18.10
- Les distributions Linux utilisant APT comme gestionnaire de paquets