Android, Fortinet, MongoDB… Les alertes sécurité de la semaine

Cisco, Red Hat, SUSE, Tenable… Autant d'éditeurs qui sont apparus cette semaine dans le fil d'avis de sécurité du CERT-FR.

Red Hat était déjà de la partie la semaine passée, pour deux vulnérabilités dans le noyau de sa distribution Linux. L'une au niveau du téléscripteur ; l'autre dans le sous-système de suivi des performances. Leur point commun : un risque de corruption de mémoire suivie d'une élévation de privilèges.
Cette fois, pas moins de huit failles. Une bonne partie concernent le sous-système iSCSI. Elles peuvent entraîner, sur RHEL 7 et 8, l'accès indésirable à des données sensibles, des dénis de services, voire des exécutions de code à distance. Les autres sont spécifiques au noyau temps réel de RHEL 8. Elle résident notamment dans le gestionnaire d'événements et dans KVM.

Les vulnérabilités iSCSI ont aussi fait l'objet d'une alerte pour **Ubuntu**. C'était mercredi. Le lendemain, le CERT-FR a attiré l'attention sur un autre noyau : celui de **SUSE** Linux Enterprise. Avec, au total, 7 failles. Elles vont de l'absence de chiffrement de trafic à la réutilisation de mémoire en passant par l'abus de Netlink par des utilisateurs sans privilèges.

Tombée mardi, la première alerte de la semaine était relative à **Tenable**. Plus précisément à Nessus, son outil d'évaluation des vulnérabilités. Le risque : qu'un utilisateur de niveau admin puisse obtenir les mêmes privilèges sur l'hôte (score CVSSv2 : 6,8).

Toujours mardi, le CERT-FR s'est fait l'écho du bulletin mensuel de sécurité d'**Android**. Au programme, une quarantaine de failles corrigées. Dont une partie touchent toutes les versions encore prises en charge (à partir, donc, d'Android 8.1). Les plus graves peuvent permettre d'exécuter du code arbitraire dans le contexte d'un processus privilégié et de modifier la localisation lors d'un appel d'urgence.

Cisco alerte sur des routeurs en fin de vie

Mercredi, ce fut au tour de MongoDB Compass. Toutes les versions sont affectées. Un tiers disposant d'un accès local au poste Windows où se trouve le logiciel peut exécuter du code avec les permissions de l'utilisateur (score CVSSv3 : 4,8).

Le même jour, Fortinet a eu droit à son alerte. Pour trois failles :

- Stockage en clair d'informations sensibles (mots de passe des utilisateurs locaux) dans un fichier de *log* de FortiADC / FortiADCManager
- Dépassement de tampon dans le démon HTTPD de FortiProxy. Un utilisateur distant authentifié peut faire planter le service au travers d'une requête PUT malformée.
- Défaut de masquage du mot de passe utilisé par Fortinet Web Vulnerability Scan pour accéder à un appareil

Android excepté, le record du nombre de failles revient à **Cisco**. Sur la base de bulletins de sécurité du 7 avril, le CERT-FR en a recensé onze. Les scores de gravité sont globalement hauts. On va jusqu'à 9,8 pour plusieurs vulnérabilités :

- L'une dans SD-WAN vManage
  Une mauvaise validation d'entrées dans le composant de gestion à distance peut entraîner un dépassement de tampon. Puis l'exécution distante de code sans authentification.
- L'autre dans les routeurs Small Business RW110W, RV130, RV130W et RV215W
  Là aussi, une mauvaise validation. Mais sur les requêtes HTTP vers la console de gestion web. Même conséquence potentielle. La différence : **il n'y aura pas de patch**, ces routeurs étant arrivés en fin de vie.

D'autres routeurs de série RV présentent des failles corrigées cette semaine. La plus critique (8,8) réside dans l'implémentation du LLDP (protocole de découverte sur la couche de liaison de données). Deux issues possibles : soit un déni de service, soit l'exécution de code par un utilisateur qui se trouve sur le même domaine de diffusion.

Illustration principale © maciek905 – Adobe Stock