

# Cisco, Ivanti, Stormshield... Les alertes sécurité de la semaine

Apple, Moodle, SUSE... Autant d'éditeurs qui sont apparus cette semaine dans le [fil](#) d'avis de sécurité du CERT-FR.

Avant eux, il y eut notamment **Ivanti**, avec une [faille](#) dans son VPN Pulse Connect Secure. Notée 8,5 sur l'échelle CVSS 3.1, elle peut permettre à un utilisateur authentifié d'exécuter du code à distance en tant que *root*. En attendant la publication d'une mise à jour, on peut importer un fichier XML qui désactivera la ressource problématique : l'explorateur de partages Windows.

On aura eu droit à une alerte SCADA, portant sur **Siemens**. Au total, [quatre failles](#), toutes créditées du même score (7,8). Elles sont liées à un mauvais traitement des fichiers ASM et PAR dans deux outils de visualisation (JT2go et Teamcenter Visualization). Les risques : l'extraction de données et l'exécution locale de code dans le contexte des processus.

Pour **Moodle**, le compteur en est à [sept failles](#). Quatre sont « sérieuses ». Elles ouvrent la voie à :

- L'exportation, par un profil enseignant, des forums de tous les cours et non seulement des siens
- La consultation, par un profil apprenant, de son score de réussite avant sa publication
- Des injections SQL sur les sites où le serveur d'échanges MNet est activé et configuré
- Des dénis de service dans la zone des brouillons, faute d'un plafonnement effectif des limites de téléversement

Comme chaque semaine ou presque, on a eu droit à des alertes CERT-FR sur les noyaux de différentes distributions Linux.

Cette fois, [essentiellement](#) SUSE. Avec plusieurs dizaines de failles dont une [de type](#) Spectre (exécution spéculative hors limites).

## Boot Camp et Raspberry Pi

Ubuntu aussi a fait l'objet d'une avis du CERT-FR. Plus précisément pour le *kernel* destiné aux Raspberry Pi. Les problèmes résolus touchent pour beaucoup à des pilotes. Entre autres Nouveau (pilote graphique ; risque de déni de service local), RLT8188EU (pilote *wireless* ; même risque) et *fastrpc* (pour les appels à distance ; risque d'élévation de privilèges).

Autre produit de sécurité signalé cette semaine : Stormshield Endpoint Security. Au menu, [une faille](#), notée 6.5. Elle pose un risque de déni de service à travers le messages de renégociation OpenSSL.

Chez Cisco, on n'est pas dans le déni de service, mais dans l'exécution distante de code (score : 8,8). [Sur trois solutions](#) : Modeling Labs, Prime Infrastructure et Evolved Programmable Network Manager. En cause, une validation insuffisante d'entrées sur l'UI web.

Chez Apple, c'est d'élévation de privilèges qu'il [s'agit](#). Produit touché : Boot Camp. Chez Mozilla, l'alerte de la semaine porte sur Thunderbird. Avec deux éléments. D'un côté, l'absence d'indication de messages partiellement protégés (contenus chiffrés *inline*). De l'autre, l'absence de chiffrement des clés OpenPGP importées sur certaines versions du client.

*Photo d'illustration © maciek905 – Adobe Stock*