SAP, Siemens, SonicWall… Les alertes sécurité de la semaine

GitLab, Microsoft, Palo Alto Networks, Schneider Electric… Autant d'éditeurs qui sont apparus cette semaine dans le fil d'avis de sécurité du CERT-FR*.

Lundi 12 avril, on a eu droit à une seule alerte. Elle porte sur **SonicWall**. Avec trois failles au programme. La plus critique affiche un score de 9,8/10 sur l'échelle CVSS. Elle réside dans l'outil d'administration GMS (Global Management System). Et présente un risque d'élévation de privilèges à distance, jusqu'au niveau root, le tout sans authentification.
Les deux autres vulnérabilités affectent Email Security. L'une peut permettre la création d'un compte admin par requête HTTP (9,4). L'autre, la création de fichiers arbitraires après authentification (6,7).

Mardi, ce fut au tour de **SAP**. Avec 14 failles, dont une créditée du score maximal. Son lieu de résidence : le navigateur Chromium embarqué dans SAP Business Client. Haut score également (9,9) pour une vulnérabilité dans SAP Commerce. Elle ouvre la voie à l'injection distante de code dans les règles sources.

Siemens et Schneider Electric au menu SCADA

Mercredi aura été une journée très « SCADA ». Avec d'une part **Schneider Electric**. Et de l'autre, Siemens. Chez le premier, il est fait état de 7 failles. Dont l'essentiel dans l'outil de configuration des installations C-Bus (automatisation). Les deux plus critiques (8,8) sont de type traversée de répertoire. Elles peuvent engendrer l'exécution de code depuis un fichier envoyé à distance.

Chez **Siemens**, pas moins de 43 failles. Nucleus est particulièrement touché. Le système d'exploitation temps réel renferme une dizaine de vulnérabilités. D'un côté, dans son module DNS (écriture hors limites, avec pour conséquences possibles un déni de service ou l'exécution de code à distance). De l'autre, la *stack* IPv6. Parmi les autres produits concernés figure Tecnomatix RobotExpert (simulation de processus), avec un score maximal de criticité de 7,8. Ainsi que SIMATIC NET (mise en réseau ; 9,8), LOGO! Soft Comfort (automatisation ; 8,4) et Siveillance (gestion de vidéosurveillance ; 9,9).

Presque autant de failles (42) chez **IBM**. Elles découlent quasiment toutes de problèmes avec Java. Infosphere Information Server fait partie des logiciels concernés, au niveau de sa couche microservices. Tivoli aussi, sur sa brique Composite Application Manager for Transactions. Il s'y trouve une faille notée 9,8. Le souci : un dépassement de pile dans Eclipse OpenJ9 lors de la conversion de caractères UTF-8. Le risque : l'exécution de code à distance.

L'Update Tuesday alourdit le bilan

Des alertes sur les navigateurs ont émaillé les journées de mercredi et de jeudi. Plus précisément sur **Chrome** et **Edge**. Partageant le même moteur de rendu, ils partagent aussi beaucoup de failles.

Dont une part importante pouvant entraîner des réutilisations indésirables de mémoire.
Dans la lignée de l'Update Tuesday, d'autres logiciels Microsoft ont fait l'objet d'avertissements du CERT-FR. En l'occurrence, Office (7 failles) et Windows (79).

GitLab et **WordPress** furent au menu du 15 avril. Avec deux failles chacun. Chez le premier, on aura relevé un score de 9,9 pour une mauvaise validation d'images dont peut résulter une exécution distante de code. Chez le second, l'API REST et la bibliothèques de médias étaient les deux composants problématiques.

Des failles, il y en a aussi chez **Palo Alto Networks**. Au nombre de quatre. La plus grave (6,7) se trouve dans le scanner de sécurité IaC Bridgecrew Checkov. Une mauvaise désérialisation des fichiers Terraform peut occasionner l'exécution locale de code malveillant. Les autres touchent GlobalProtect (déni de service *via* le pilote VPN ; 5,5) et PAN-OS (divulgation de secrets).

** On consultera ces différents avis de sécurité pour avoir la liste précise des versions affectées de chaque logiciel.*