

# Une partie de l'Internet mondial mise à l'arrêt

Des pages ont été mises en maintenance par précaution, ce mercredi, en raison d'une faille de sécurité.

« **MAINTENANCE** en cours. » En milieu d'après-midi ce mercredi, de nombreux sites d'institutions (préfectures de police, Santé publique France, Météo France, Impôts) ou de médias (« les Échos », « Challenges ») ont été rendus inaccessibles. Et la France n'est pas un cas isolé : dans d'autres pays aussi, des pages Web étaient hors service.

Tout s'explique par deux vulnérabilités « critiques » détectées dans PHP, un langage de programmation utilisé par près de 75 % des sites Web, et annoncées mardi soir.

Le ministère de l'Intérieur fait ainsi savoir qu'il « a procé-

dé, à la demande de l'Agence nationale de la sécurité des systèmes d'information, à la mise en maintenance préventive de l'ensemble de ses sites exposés à une vulnérabilité critique de sécurité, annoncée il y a quelques heures par l'éditeur d'un composant logiciel générique, largement utilisé à travers le monde ». L'agence américaine de renseignement NSA a fait la même recommandation.

« La première vulnérabilité découverte concerne le téléchargement d'un document sur un site. Un fichier malveillant pourrait permettre à un hacker de mener une exé-

cution de code à distance (RCE) sur un serveur, explique Guillaume Vassault-Houlière, PDG de YesWeHack. Il pourrait alors récupérer des mots de passe et des identifiants, et rebondir vers une base de données à voler. »

## « Une vulnérabilité rare »

La mise à jour a été rendue disponible à 16 heures, ce mercredi. « C'est une mesure de précaution en attendant le patch de sécurité, confirme Guillaume Vassault-Houlière. Sans cette mise à jour, un site est vulnérable. L'exploitation d'une telle faille prenait plusieurs jours après sa décou-

verte, mais avec l'intelligence artificielle, tout s'accélère et développer une attaque ne prend qu'une minute. Le coût d'entrée d'une telle opération a aussi baissé. » Dès lors, « le plus simple est de mettre tout hors ligne afin de protéger ses données et d'évacuer le vecteur d'attaque, le trou béant, avec une mise à jour avant de tout redémarrer », ajoute-t-il.

Pendant combien de temps ? À 20 heures ce mercredi, de nombreux sites (comme ceux de Météo France et de Santé publique France) étaient actifs, mais d'autres pas encore. La durée de maintenance dépend de l'état du

parc de serveurs, et souvent de prestataires extérieurs.

« Beaucoup de sites sont clients de fournisseurs de solutions Web qui gèrent des millions de références. D'autres ne savent même pas quels serveurs sont sur PHP. Ce n'est pas très technique, mais plutôt une question de recensement de vieilles machines à mettre à jour », analyse Clément David, PDG de Theodo Cloud, une entreprise de services du numérique.

À ce stade, il n'y a pas de raison de paniquer. Mais il était urgent d'agir. « Nous sommes face à une vulnérabilité rare qui tombe sur une technologie

populaire, vieille et d'ordinaire robuste, avance Guillaume Vassault-Houlière. Elle a été trouvée dans le code source et si rien ne garantit qu'elle sera exploitée, elle doit être immédiatement éliminée. »

Reste à voir dans les jours qui viennent si des données ayant fuité de tel ou tel site n'apparaissent pas sur Internet... « Nous observons l'émergence d'attaques précoces », a déjà prévenu mercredi matin Dane Knecht, directeur technique de l'entreprise spécialisée en cybersécurité Cloudflare.

**N. B et Damien Licata Caruso**