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

FAILLES CRITIQUES DANS

LE CMS DRUPAL

Contenu

I. Contexte

Les développeurs de Drupal, un logiciel de gestion de contenu open source populaire qui alimente des millions de sites Web, ont publié la dernière version de leur logiciel afin de corriger une vulnérabilité critique qui pourrait permettre à des attaquants distants de pirater votre site.

Drupal est le troisième CMS le plus populaire pour l'édition de sites Web, représentant environ trois pour cent des milliards de sites Web dans le monde. Les pirates pourraient utiliser ladite faille, identifiée par le numéro CVE-2019-6340, pour pirater un site Drupal et potentiellement prendre le contrôle d'un serveur Web.

II. Analyse

La vulnérabilité en question est une faille critique d'exécution de code à distance (RCE) dans Drupal Core qui pourrait « conduire à l'exécution de code PHP arbitraire dans certains cas », le bogue est dû à certains types de fichiers qui ne traitent pas correctement les données provenant d'autres formulaires. La mise à jour a eu lieu deux jours après que l'équipe de sécurité de Drupal ait publié une notification de sécurité concernant les correctifs à venir, permettant aux administrateurs de sites Web de résoudre rapidement leurs problèmes avant que les pirates informatiques n'exploitent cette faille.

Bien que l'équipe Drupal n'ait publié aucun détail technique sur la vulnérabilité (CVE-2019-6340), elle a indiqué que la faille réside dans le fait que certains types de champs ne nettoient pas correctement les données provenant de sources non vérifiées et affectent Drupal 7 et 8. Il convient également de noter que votre site Web basé sur Drupal n'est affecté que si le module Services Web RESTful est activé et permet les requêtes PATCH ou POST, ou si un autre module de services Web est activé.

III. Correctifs

Si vous ne pouvez pas installer immédiatement la dernière mise à jour, vous pouvez atténuer cette vulnérabilité en désactivant simplement tous les modules de services Web ou en configurant votre ou vos serveurs Web pour interdire les requêtes PUT / PATCH / POST aux ressources de services Web. Cependant, compte tenu de la popularité des exploits Drupal parmi les pirates, il est fortement recommandé d'installer la dernière mise à jour :

- Si vous utilisez Drupal 8.6.x, mettez à niveau votre site Web vers Drupal 8.6.10.
- Si vous utilisez Drupal 8.5.x ou une version antérieure, mettez à niveau votre site Web vers Drupal 8.5.11.

Drupal a également déclaré que le module de services Drupal 7 ne nécessitait pas de mise à jour, mais les utilisateurs devraient néanmoins envisager d'appliquer d'autres mises à jour associées au dernier avis.