الجمهوريـــة الجـزائريـة الديمـقراطيـة الشـعبية
وزارة التعليم العالي والبحث العلمي
مديرية الشبكات وأنظمة الإعلام والاتصال الجامعية
المديرية الفرعية للأمن المعلوماتي
Site web: www.mesrs.dz
Courrier électronique: sdsi@mesrs.dz
Alger le 10/07/2016 الجزائر
المرجع: DRSICU/SDSI/16/54

NOTICE DE SECURITE N° 37/2016 du 10 juillet 2016

A Messieurs les Présidents des Conférences Régionales

A Mesdames et Messieurs les Chefs d'établissement

Objet : Failles de sécurité critiques dans les sites développés avec Drupal et avec WordPress et dans Adobe Flash Player.

J'ai l'honneur de vous faire part de la notice de sécurité établie à la suite de la découverte des multiples vulnérabilités critique dans le ***CMS Drupa et CMS WordPress et dans Adobe Flash Player***.

I. CMS Drupa :

Les versions du CMS Drupal affectées :

- Drupal core 7.x versions antérieures à 7.44
- Drupal core 8.x versions antérieures à 8.1.3.

1. RISQUES :
- contournement de la politique de sécurité,
- élévation de privilèges.

2. CORRECTION - PARADE:
Mise à niveau vers :

- ✓ Drupal core 7.44 pour Drupal 7.x,
- ✓ Drupal core 8.1.3 pour Drupal 8.x.

3. SOURCES:

Drupal:
https://www.drupal.org/SA-CORE-2016-002

II. CMS WordPress :

Toutes les versions du CMS WordPress antérieures à 4.5.3 sont affectées par deux failles de sécurité

1. RISQUES :

- déni de service à distance,
- contournement de la politique de sécurité,
- atteinte à l'intégrité des données,
- atteinte à la confidentialité des données,
- injection de code indirecte à distance.

2. CORRECTION - PARADE:

La mise à jour régulière du CMS WordPress est indispensable pour assurer la sécurité de vos sites web (WordPress 4.5.3 corrige 17 failles de sécurité).

3. SOURCES:

WordPress :

https://wordpress.org/news/2016/06/wordpress-4-5-3/

III. Adobe Flash Player :

Les versions du Adobe Flash Player affectées :

- Adobe Flash Player Desktop Runtime versions antérieures à 22.0.0.192 sur Windows et Macintosh
- Adobe Flash Player ESR versions antérieures à 18.0.0.360 sur Windows et Macintosh
- Adobe Flash Player pour Google Chrome versions antérieures à 22.0.0.192 sur Windows, Macintosh, Linux et ChromeOS
- Adobe Flash Player pour Microsoft Edge et Internet Explorer 11 versions antérieures à 22.0.0.192 sur Windows 10 et 8.1
- Adobe Flash Player versions antérieures à 11.2.202.626 sur Linux
- Adobe Flash Player 21.0.0.242 et versions antérieures pour Windows, Macintosh, Linux et Chrome OS.

1. RISQUES :

- exécution de code arbitraire à distance,

- prendre le contrôle du système affecté.

2. CORRECTION - PARADE:

Mettre à jour Adobe Flash Player vers les dernières versions stables.

3. SOURCES:

Adobe Flash Player:

- https://helpx.adobe.com/security/products/flash-player/apsa16-03.html
- https://helpx.adobe.com/security/products/flash-player/apsb16-18.html

DIFFUSION: La sécurité est l'affaire de tous, dans l'intérêt de tout le monde, merci d'assurer la diffusion de ces informations la plus large entre et dans les établissements.

Salutations cordiales.