Bulletin d'alerte de sécurité du CSIRT DOCAPOST

Vulnérabilité dans Drupal Core 6.x / 7.x / 8.x
CSIRT-DCP-ALE-2018-003

GESTION DU DOCUMENT

Date de la première version :	28/03/2018
Date de la dernière version :	30/03/2018
Version :	1.2
	ANSSI / CERT-FR
Source :	C.O.S.C / CSIRT DOCAPOST
	SLCC / CERT La Poste

RISQUE(S) / IMPACT(S)

Score CVSS

Score de base :	9.6	AV:**Réseau** / AC:**Bas** / Au:**Aucun** / C:**Complète** / I:**Complète** / A:**Complète**
Score temporel :	X.X	E:**X** / RL:**X** / RC:**X**
Score Environmental :	X.X	CDP:**XX** / TD:**X** / CR:**X** / IR:**XX** / AR:**XX**

Risque(s) :

- Exécution de code arbitraire à distance

Impact(s) :

- Perte de la confidentialité de la donnée
- Perte de l'intégrité de la donnée
- Perte de la disponibilité de la donnée

RESUME DE LA VULNERABILITE OU DE LA MENACE

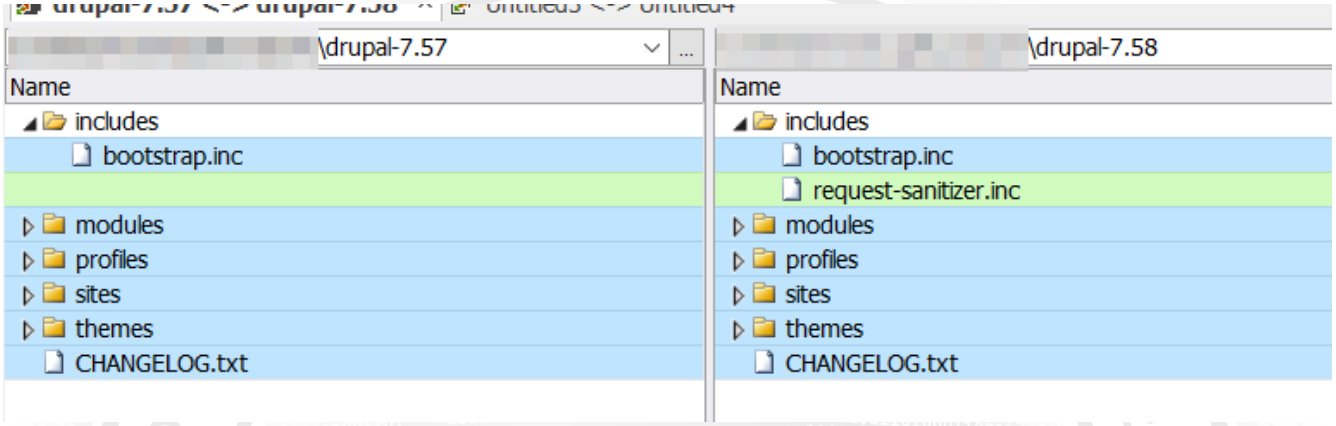
Le 28 mars 2018, l'éditeur du système de gestion de contenu Drupal a publié un avis de sécurité concernant une vulnérabilité critique dans Drupal core. L'avis SA-CORE-2018-002 indique que les systèmes Drupal en versions 7.x, 8.5.x, mais également les systèmes n'étant plus supportés (version 8.3.x, 8.4.x et 6), sont affectés par une vulnérabilité hautement critique pouvant mener à la compromission complète d'un site web basé sur Drupal.

Cette vulnérabilité, identifiée en tant que CVE-2018-7600, permettrait à un visiteur d'un site vulnérable d'accéder à toutes les données contenues sur le site, de les modifier et de les supprimer, et ce sans authentification.

Le C.O.S.C recommande d'appliquer au plus tôt les correctifs de sécurité mis à disposition par Drupal ou d'appliquer les contre-mesures réactives.

VECTEUR(S) D'INFECTION(S) / D'ATTAQUE(S)

L'avis de sécurité ne mentionne pas tous les détails concernant la vulnérabilité, et aucun exploit disponible publiquement n'a encore été détecté sur les réseaux. Cependant, en raison de la nature de Drupal (Open-Source), nous pouvons comprendre le contexte du changement en utilisant le commit Git ; Le changement de code montre une bibliothèque ajoutée au code: request-sanitizer.inc. La fonction principale de la bibliothèque est appelée "stripDangerousValues".



Cela donne un indice évident qu'il existe des problèmes de sanitization des entrées utilisateur avec Drupal. Cela signifie que l'entrée de l'utilisateur risque d'être évaluée de façon non sûre dans des méthodes d'exécution de code non protégées. En d'autres termes, une exécution de code à distance arbitraire et plus.

Par conséquent, un exemple d'exploit peut ressembler à ce qui suit:

```
index.php? page ['# payload'] = home.php
```

SYSTEME(S) AFFECTE(S)

- Drupal Core :
  - Drupal versions 8.5.x antérieures à 8.5.1
  - Drupal versions 8.4.x antérieures à 8.4.6
  - Drupal versions 8.3.x antérieures à 8.3.9
  - Drupal versions 7.x antérieures à 7.58
  - Drupal version 6

RESUME

Une vulnérabilité d'exécution de code arbitraire à distance existe dans plusieurs sous-systèmes de Drupal 7.x et 8.x. Cela permet potentiellement aux attaquants d'exploiter plusieurs vecteurs d'attaque sur un site Drupal, ce qui pourrait entraîner la compromission complète du site.

CONTRE(S) MESURE(S)

Mise à jour Drupal Core

- Mettre à niveau vers la version la plus récente de Drupal 7 ou 8 core.
  - Si vous utilisez 7.x, passez à Drupal 7.58. (Si vous ne parvenez pas à effectuer la mise à jour immédiatement, vous pouvez essayer d'appliquer ce correctif pour corriger la vulnérabilité jusqu'à ce que vous puissiez effectuer une mise à jour complète.)

- Si vous exécutez 8.5.x, effectuez une mise à niveau vers Drupal 8.5.1. (Si vous ne parvenez pas à effectuer la mise à jour immédiatement, vous pouvez essayer d'appliquer ce correctif pour corriger la vulnérabilité jusqu'à ce que vous puissiez effectuer une mise à jour complète.)

Drupal 8.3.x et 8.4.x ne sont plus supportés. L'éditeur ne fournies généralement pas les versions de sécurité pour les versions mineures non supportées. Cependant, étant donné la gravité potentielle de ce problème, l'éditeur fournies des versions 8.3.x et 8.4.x qui incluent le correctif pour les sites qui n'ont pas encore eu la possibilité de passer à la version 8.5.0.

La page de rapport de mise à jour du CMS recommandera la version 8.5.x même si vous utilisez le format 8.3.x ou 8.4.x. Veuillez prendre le temps de mettre à jour vers une version prise en charge après l'installation de cette mise à jour de sécurité.

Si vous exécutez 8.3.x, effectuez une mise à niveau vers Drupal 8.3.9 ou appliquez ce correctif. Si vous exécutez 8.4.x, mettez à niveau versDrupal 8.4.6 ou appliquez ce correctif.

Ce problème affecte également Drupal 8.2.x et les versions antérieures, qui ne sont plus prises en charge. Si vous exécutez l'une de ces versions de Drupal 8, mettez à jour vers une version plus récente, puis suivez les instructions ci-dessus.

Ce problème affecte également Drupal 6. Drupal 6 est en fin de vie. Pour plus d'informations sur le support Drupal 6, veuillez contacter un fournisseur D6LTS.

MESURE(S) REACTIVE(S)

En cas d'impossibilité de la mise à jour du noyau Drupal voici les contre-mesures réactives à déployer sur un système Apache avec mod_Security et les Firewall Web Applicatif du constructeur F5 ASM

Mod_Security

```
# SPECIFIC: Block #submit #validate #process #pre_render #post_render #element_validate
#after_build #value_callback parameters

SecRule REQUEST_FILENAME "(index\.php|\/$)"
"chain,id:003294,t:lowercase,t:none,t:utf8toUnicode,t:urlDecodeUni,t:urldecode,block"
      SecRule REQUEST_METHOD "^(GET|POST|HEAD)$" chain
      SecRule ARGS_NAMES|REQUEST_COOKIES_NAMES "^\#
(submit|validate|pre_render|post_render|element_validate|after_build|value_callback|process)
$|\ [(?:\'|\")?#
(submit|validate|pre_render|post_render|element_validate|after_build|value_callback|process)"

# GENERIC: Block all parameters starting with #
SecRule REQUEST_FILENAME "(index\.php|\/$)"
"chain,id:003309,t:lowercase,t:none,t:utf8toUnicode,t:urlDecodeUni,t:urldecode,block"
      SecRule REQUEST_METHOD "^(GET|POST|HEAD)$" chain
      SecRule ARGS_NAMES|REQUEST_COOKIES_NAMES "^\#|\[(?:\'|\")?\#.*\]"
```

F5 ASM Mitigation

ASM est capable de détecter ce vecteur d'attaque en utilisant la signature "SQL-INJ" '# "(commentaire SQL) (Paramètre)":

Detected Keyword	page['#payload']=home.php
Attack Signature	**Signature ID** 200002305 **Signature Name** SQL-INJ '" #" (SQL comment) (Parameter)
Context	Parameter (detected in Query String)
Parameter Level	Global
Actual Parameter Name	page['#payload']
Wildcard Parameter Name	*
Parameter Value	home.php
Applied Blocking Settings	Alarm Learn

Néanmoins, une ASU contenant des signatures spécifiques à cette vulnérabilité a été publié et prête à être téléchargée.

Latest Update Details

Create Date	2018-03-29 19:09:26
Update Date	2018-03-30 04:04:33
Updated By	ASM User Interface
Updated Mode	Scheduled
Added Signatures	45 (View Details)
Signatures with major updates	8 (View Details)
Signatures with minor updates	70 (View Details)
	Hide Readme Update: v11.6.1/ASM-SignatureFile_20180329_190926: Added Server Side Code Injection signature 200004423 for Drupal Core RequestSanitizer Remote Code Execution (1) Added Server Side Code Injection signature 200004424 for Drupal Core RequestSanitizer Remote Code Execution (2) Added Server Side Code Injection signature 200004425 for Java code injection - org.apache.tomcat.dbcp.dbcp2.BasicDataSource (Parameter) Added Server Side Code Injection signature 200004426 for Java code injection - org.apache.tomcat.dbcp.dbcp2.BasicDataSource (Header) Added Server Side Code Injection signature 200004427 for Java code injection - org.apache.tomcat.dbcp.dbcp2.BasicDataSource

Base de signature ASM DOCAPOST Confiance

IOC

- Aucun à la rédaction de l'alerte

DOCUMENTATIONS ET INFORMATIONS TECHNIQUES

- PSA-2018-001
- SA-CORE-2018-002
- CVE-2018-7600
- Foire aux questions sur la vulnérabilité CVE-2018-7600
- Security risk levels defined

CONTACTS