



1<sup>er</sup> Clasificado  
Internacional  
#CyberEX17



Entelgy

# Notificación Vulnerabilidad Crítica en Drupal



La confianza de vivir **(ciber)** seguro



Descubra nuestro  
video corporativo



[www.innotecsystem.com](http://www.innotecsystem.com)

Argentina | Brasil | Chile | Colombia | España | México | Perú



## Vulnerabilidad crítica en Drupal: actualizar inmediatamente

El **CSIRT** de **InnoTec**, empresa de ciberseguridad del **Grupo Entelgy**, alerta sobre la publicación de una vulnerabilidad crítica en **Drupal (versiones 6x, 7x y 8x)** que permite a un atacante ejecutar código en la página web que emplee este gestor de contenido (CMS) y tomar el control de la misma, así como acceder al servidor utilizado.

El equipo de Drupal (uno de los gestores de contenidos más utilizados en la actualidad, presente en más de un millón de sitios web de todo el mundo) ha publicado una actualización que corrige esta vulnerabilidad. Se recomienda implantar inmediatamente el parche para evitar quedar expuestos a posibles exploits (una vez conocidos los detalles de la actualización es de esperar que en poco tiempo se desarrollen bots que detecten los sistemas vulnerables).

### Productos afectados

La vulnerabilidad, cuyo identificador es **CVE-2018-7600**, afecta a las versiones de Drupal 7x y 8x, así como a Drupal 6 (fuera de soporte desde el año 2016) y que permite a un atacante ejecutar código en la página web que emplee este gestor de contenido (CMS) y tomar el control de la misma, así como acceder al servidor utilizado.

Los propios desarrolladores de esta plataforma ya informaron el pasado 21 de marzo de la existencia de este fallo y confirmaron que estaban preparando una actualización que lo solucionara para este miércoles, 28 de marzo, como así ha sido.

### Mitigación

Para evitar estar expuestos es necesario la instalación inmediata de la versión más reciente del Drupal:

- Si utiliza Drupal 8.3.x, actualice a la versión 8.3.9 (recuerde que esto son versiones ya no compatibles)
- Si utiliza Drupal 8.4.x, actualice a la versión 8.4.6 (recuerde que esto son versiones ya no compatibles)
- Si utiliza Drupal 8.5.x, actualice a la versión 8.5.1
- Si utiliza Drupal 7.x, actualice a la versión 7.58
- Si utiliza Drupal 6.x contacte con un mantenedor de Drupal 6 LTS.

InnoTec recomienda, además, realizar una copia de seguridad de seguridad de la base de datos y de todos los ficheros que componen el sitio web, incluida una copia del fichero de configuración del portal.

### Más información:

Drupal:

<https://www.drupal.org/sa-core-2018-002>

<https://groups.drupal.org/security/faq-2018-002>

### Contacto

**CSIRT Entelgy (InnoTec)**

[csirt@entelgy.com](mailto:csirt@entelgy.com)



Avenida Llano Castellano, 43 28034, Madrid

+34 917 281 504 - <http://www.innotecsystem.com>