Restricting access to /downloader/ in Magento

rdavis@foregenix.com - 2019-05-02 - Comments (0) - Magento

We are noticing more and more customers who come to us for an investigation have their **`/downloader/`** directory publicly accessible to anyone and everyone. Typically, this provides an attacker a surface to penetrate and often enough they'll use a brute-force attack to make their way into the **`/downloader/`** area of Magento.

The Magento Connect Manager is available via **`/downloader/`** location and is used for the installation of Magento Extensions, Magento upgrades and requires Magento admin rights for this. The authorization method used is the same as the one for the backend. Therefor if a matching pair of credentials are indeed identified the whole Magento installation will be compromised.

What can be done in order to prevent this?

There are many ways we can restrict access to the /downloader/ directory. Please see some examples below.

Move /downloader/ out when it is not needed

The simplest way to prevent access to the **`/downloader/`** directory which requires no previous knowledge of web servers, file systems, permissions, etc is to simply move or even remove the folder. To do this, make your way to your Magento root directory via your control panel, FTP, SFTP and simply move the **`/downloader/`** folder into another folder which is already protected or even remove it from the web root and store it offline. Then, when you need to use the Magento Connect Manager, simply put the folder back.

Restrict access by implementing additional password protection

Create a password protection file under the **`var/`** directory, for example **`var/.htpasswd`**, using the htpasswd command on your server.

Apache2 with .htaccess enabled

Add the following lines at the top of the **`/downloader/.htaccess`** file:

```
AuthType Basic
AuthName "Restricted"
AuthUserFile /path/to/root/var/.htpasswd
Require valid-user
```

Nginx

Your nginx configuration file for the website should be under **`/etc/nginx/sites-available/`**. Add the two entries below under for the domain path that you want to secure. If you don't have access to your nginx configuration file your hosting provider will.

```
location /downloader/ {
  auth_basic           "Restricted";
  auth_basic_user_file /path/to/root/var/.htpasswd;
  }
```

Restrict access via specific IP's

Apache2 with .htaccess enabled

Add the following lines to the top of your **`/downloader/.htaccess`** file:

```
Order deny,allow
Deny from all
Allow from 127.0.0.1 #IP's you wish to allow
```

127.0.0.1 is an example IP-address, please make sure to add your IP-address and any another administrators who use Magento Connect, install extensions or perform upgrades as they won't be able to access the **`/downloader/`** directory.

Nginx

Your nginx configuration file (nginx.conf) for the website should be under **`/etc/nginx/sites-available/`**. Add the two entries below under for the domain path that you want to secure. If you don't have access to your nginx configuration file your hosting provider will.

```
location /downloader/ {
  allow 127.0.0.1;
  deny all;

}
```

Tags

access

access configuration

configuration

downloader

hide

Magento

Restrict

Secure