PrestaShop

Module vulnerability - related to PHPUnit dependency

Latest update: 07/01/2020

Follow up

We have released an official statement with updated informations here.

This document will not be updated anymore, new information will be published on the PrestaShop blogs.

Background

Thursday 2nd of January 2020, a customer reported that its shop has been compromised by a malware named XsamXadoo Bot. The bot was able to upload some malware files into the shop which allowed him to access and control several shop settings.

After some research, we believe that the bot was able to upload those malware using a known vulnerability of the PHP tool PHPUnit that has been reported as CVE-2017-9841.
See https://nvd.nist.gov/vuln/detail/CVE-2017-9841

PHPUnit is a tool we use to build prestashop modules, but it should only be used on a developer computer. So it is very unlikely the vulnerable files will be found on a server and make the server vulnerable.

Unlikely but not impossible. These files have wrongly been added into some prestashop module ZIP archives. If a shop has downloaded one of these compromised archives, and has not deleted it since, then the shop is now vulnerable.

We can confirm that there are multiple shops running that are vulnerable right now (= can be attacked at any time) and multiple shops running that are already compromised.

How to find if my shop is vulnerable ?

Please look into the modules/ directory of your shop, and for each module in this directory, check whether it contains a directory “vendor” and inside this “vendor” directory, there is another directory with name “phpunit”.

If one module contains this vendor/phpunit directory, this module might make you vulnerable and allow an outside attacker to upload malware files into your shop.

How to protect my shop if a module makes it vulnerable ?

If you have found than one module on your shop contains the vendor/phpunit directory, you can simply delete the vendor/phpunit directory. It is not necessary for the module correct behavior. This simple step will protect your shop from this vulnerability.

On a Linux server, the cleanup procedure to fix a vulnerable shop can be performed using the following bash command line from the modules/ folder from the shop:

```
find . -type d -name "phpunit" -exec rm -rf {} \;
```

This command requires the relevant user rights.

However you must also check whether, while your shop was vulnerable, it has been compromised.

How to find if my shop has been compromised ?

This vulnerability allows an attacker to execute PHP code on your shop.
This means that an attacker
-can read the content of your database to steal data
-can upload files on your server
-can modify files on your server

The stolen data cannot be retrieved and there is no reliable way to check whether your data has been stolen.
However you should be able to find out whether some files have been added or modified.
In the case that was reported, the XsamXadoo Bot, we have been able to spot undesired files with name XsamXadoo_Bot.php on the server. It is needed to remove them.
Following this example you need to track and remove compromised files on your server.

What is PrestaShop doing right now about this vulnerability ?

Right now, we are checking every PrestaShop module archives to track whether or not they contain the vendor/phpunit vulnerable directory. We will remove or patch all archives which contain this vulnerable directory, then communicate the list of the vulnerable module versions and how to protect shops.

List of vulnerable archives

We have found that the following ZIP archives contained the vulnerable files:

Downloadable from GitHub

https://github.com/PrestaShop/autoupgrade/releases/download/v4.3.0/autoupgrade-v4.3.0.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.2.0-beta.1/autoupgrade-v4.2.0-beta.1.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.1.1/autoupgrade-4.1.1.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.1.0/autoupgrade-v4.1.0.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.1.0-beta.2/autoupgrade-v4.1.0-beta.2.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.1.0-beta.1/autoupgrade-v4.1.0-beta.1.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.0.0/autoupgrade-v4.0.0.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.0.0-beta.4/autoupgrade-v4.0.0-beta.5.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.0.0-beta.4/autoupgrade-v4.0.0-beta.4.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.0.0-beta.3/autoupgrade-v4.0.0-beta.3.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.0.0-beta.2/autoupgrade-v4.0.0-beta.2.zip
https://github.com/PrestaShop/autoupgrade/releases/download/v4.0.0-beta.1/autoupgrade-v4.0.0-beta.1.zip

All these packages have been deleted from GitHub.

Distributed through PrestaShop API

Modules released with vulnerable version of PHPUnit:

- module pscartabandonmentpro ; versions v2.0.1 and 2.0.2 (PHPUnit v4.8.36)
- module ps_facetedsearch ; version v2.2.1 (PHPUnit v5.0.9)

Modules released with recent version of PHPUnit:

- module ps_checkout ; versions v1.0.8 & v1.0.9 (PHPUnit v5.7.27)
- module ps_facetedsearch ; version v3.0.0 (PHPUnit v5.7.27)
- module autoupgrade ; versions 4.x (PHPUnit v5.7.27)

Currently unknown status:
- - module gamification ; versions being searched

If we find additional vulnerable archives, we will add them to this list.