

On 15.09.2022 we received info from PrestaHome Developer who is creator of Simple Blog module which is included In Warehouse Theme thanks to extended license. He informed us about SQL injection vulnerability found in his module.

”

*Dear partners,*

*A few days ago, we got a message that Blog for PrestaShop is vulnerable to SQL Injection attacks. It is information based on the dedicated audit performed by one of the French PrestaShop agencies for their customer, and it is not public yet.*

*We've performed a full audit of the code and sent an upgraded version (1.8.0) of the module to the Envato Marketplace. After release (you'll get an email from Envato), please upgrade it as soon as possible.*

*Front-office part of the module is fully compatible with the previous versions.*

*If you can't update the entire module, please make sure to update /controllers/front/list-v17.php. Still, without backward-incompatible changes, there should be no problems with the upgrade path, and we highly recommend upgrading the module entirely.*

*The module should be fully compatible with PrestaShop 1.6, 1.7, and with the new version, 8.0, but we are no longer officially supporting PrestaShop 1.6.*

*If you have any questions, please let us know.*

--

*Best regards,  
PrestaHome Support Team*

”

We applied fix In latest Warehouse version 4.5.5 which we realased few hours after receiving information.

If you can not upgrade theme to latest version, you shpuld follow Blog module developer advice and upgrade only one affected file which will fix the issue and will have no impact on other parts of your theme

The file is

*/Ph\_simpleblog/controllers/front/list-v17.php*

You can find the file In „Simple blog security fix” folder and you need to copy it by ftp

To

**/modules/ph\_simpleblog/controllers/front/list-v17.php**

*\*( make sure you copy and replace it In path /modules/ph\_simpleblog/controllers/front/list-v17.php and not In themes/warehouse/modules/ph\_simpleblog/controllers/front/list-v17.php)*