Checklista _
Jak zabezpieczyć sklep PrestaShop przed atakami hakerskimi i co zrobić, gdy już nastąpił włam

Wstęp

Hej! Jesteśmy Convertis! - Software House oferujący wsparcie programistycznie dla sklepów opartych o technologię PrestaShop.

W okresie lipiec/sierpień 2022 spotkaliśmy się z procederem włamów na tej platformie u Klientów.

W naszej firmie jedną z najważniejszych rzeczy (zaraz po Ludziach) są procesy i instrukcje. Pozwalają nam one efektywnie, sprawnie, ale przede wszystkim skutecznie działać.
Tym razem stworzyliśmy narzędzie, z którego sami korzystamy pomagając sklepom przy kolejnych potencjalnych lub wykrytych przypadkach włamów.

I teraz chcemy się nim z Wami podzielić, abyście mogli z niego skorzystać, kiedy przydarzy Wam się atak hakerski.

Ten dokument cały czas będziemy aktualizować według naszej najnowszej wiedzy, kolejnych przypadków (miejmy nadzieję, że się nie zdarzą), a także doniesień z branży.
To roboczy skrypt, oparty na naszym doświadczeniu, także, jeśli uważasz, że trzeba coś w nim zmienić, poprawić lub uzupełnić o jakieś info czy działania daj znać na: Hello@convertis.pl lub na https://convertis.pl/kontakt/

Będziemy wdzięczni!
Mamy nadzieję, że będzie to z korzyścią dla całej branży!

Poniżej lista rzeczy “must have”, które musisz wykonać, aby zapobiec włamaniom.
Oczywiście postępowanie po włamaniu powinno również objąć te prace.
Lista jest stworzona po to, żeby zabezpieczyć się, zanim ktoś będzie chciał zaatakować Twój ecommerce.

v1.0 z dnia 220816

Checklista

1. Zachowaj spokój!

2. Zapoznaj się z oficjalną informacją opublikowaną przez PrestaShop dotyczącą właśnie ataków. Już w niej firma wskazuje jakie kroki powinniśmy podjąć.
   https://build.prestashop.com/news/major-security-vulnerability-on-prestashop-websites/.
   Ataki były realizowane poprzez dziurę sqlInjection i mechanizm cache'owania templatek smarty w MYSQL, co pozwalało na wstrzyknięcie złośliwego kodu do templatek.

3. Twój Klient, albo Ty używacie używa modułu **blockwishlist> 2.0.0?**
   Jeśli tak, to zaimplementuj patch:
   https://github.com/PrestaShop/blockwishlist/commit/b3ec4b85af5fd73f74d55390b226d221298ca084

4. Korzystasz z **PrestaShop 1.7>1.7.8.2?**
   Jeśli tak, zaimplementuj patch presty na orderby:
   https://github.com/PrestaShop/PrestaShop/commit/6482b9ddc9dcebf7588dbfd616d2d635218408d6

   Jeśli korzystasz z PrestaShop 1.6 też możesz zaimplementować modyfikacje metody ValidateCore::isOrderBy z powyższego commita.

5. Przeanalizowane przez nas przypadki wskazują na to, że atakujący wykorzystują mechanizm cache smarty w MYSQL, więc zablokuj tę opcję kasując w pliku **config/smarty.config.inc.php** linijki:

   ```
   if (Configuration::get('PS_SMARTY_CACHING_TYPE') == 'mysql') {

   include _PS_CLASS_DIR_.'Smarty/SmartyCacheResourceMysql.php';

   $smarty->caching_type = 'mysql';

   }
   ```

6. Przejrzyj zabezpieczenia katalogów:
   - **upload, img, var, vendor** itp.
   upewnij się czy posiadają **.htaccess, index.php** oraz czy blokują wykonanie **php** wszędzie tam gdzie nie jest to wymagane.
   Jeśli napotkasz tu braki, koniecznie uzupełnij je.
   a. Trzeba wziąć pod uwagę czy .htaccess jest wykonywany przez Twój serwer http. Jeśli używasz np. serwera nginx, który nie wykonuje reguł .htaccess - zgłoś się do administratora o sprawdzenie zabezpieczeń.

b. Jeśli napotkasz bałagan, czy zauważysz dziwne pliki, katalogi, bądź niepotrzebne moduły - uporządkuj je. Całą niepotrzebną zawartość przenieś do archiwum niedostępnego przez http.

7. Zweryfikuj wdrożenie poprawek z listy:

https://www.cvedetails.com/cve/CVE-2021-21308/ poniżej 1.7.7.2

https://www.cvedetails.com/cve/CVE-2020-4074/ poniżej 1.7.7.2

https://www.cvedetails.com/cve/CVE-2021-3110/ - product comment 5.0.0 -> zrób upgrade do 5.0.1

https://www.cvedetails.com/cve/CVE-2020-26248/ product comment (jeśli w sklepie jest moduł poniżej 4.2.1

https://www.cvedetails.com/cve/CVE-2020-15160/ 1.7.5 - 1.7.6.8

https://www.cvedetails.com/cve/CVE-2018-20717/ poniżej 1.7.2.5

https://www.cvedetails.com/cve/CVE-2018-19355/ dotyczy wersji 1.6

https://www.cvedetails.com/cve/CVE-2018-19126/ dotyczy poniżej 1.6.1.23 i poniżej 1.7.4.4

https://www.cvedetails.com/cve/CVE-2018-8824/ dotyczy modułu BAMEGAMENU

https://www.cvedetails.com/cve/CVE-2018-8823/ dotyczy modułu BAMEGAMENU:

8. Przeskanuj serwer narzędziem antywirusowym - możesz użyć: https://github.com/marcocesarato/PHP-Antimalware-Scanner lub zleć to administratorowi.

9. Sprawdź uprawnienia obsługi w panelu administracyjnym - powinno być tylko jedno konto z uprawnieniami superadministratora. Bieżącą pracę zawsze należy wykonywać na koncie bez uprawnień do wgrywania plików modułów, templatek i tłumaczeń.

Jeśli chcesz być na bieżąco z aktualizacjami listy napisz do nas: hello@convertis.pl, będziemy Cię informować o każdej jej zmianie.