Уязвимость в PHP7 подвергает сайты риску удаленного взлома

В ветке PHP 7 выявлена опасная уязвимость (CVE-2019-11043), предоставляющая злоумышленникам возможность выполнять команды на сервере, используя специально сформированный URL.

Проблема распространяется исключительно на NGINX-серверы с включенным PHP-FPM (программный пакет для обработки скриптов на языке PHP). Уязвимыми являются конфигурации nginx, где проброс в PHP-FPM осуществляется с разделением частей URL при помощи "fastcgi_split_path_info" и определением переменной окружения PATH_INFO, но без предварительной проверки существования файла директивой "try_files $fastcgi_script_name" или конструкцией "if (!-f $document_root$fastcgi_script_name)".

Разработчики выпустили патч для данной уязвимости в минувшую пятницу, 25 октября. Всем пользователям настоятельно рекомендуется обновиться до новейших версий PHP 7.3.11 и PHP 7.2.24.

Подробнее: https://www.securitylab.ru/news/502087.php