

## Об уязвимости в ядре Linux



Web-серверы на Linux и миллионы Android-устройств находятся в зоне риска в связи с уязвимостью в ядре Linux, которая затрагивает генератор псевдослучайных чисел и позволяет осуществлять межуровневые атаки благодаря тому, что алгоритмы генерации UDP, IPv6 и IPv4, работающие на некоторых Linux-системах, используют уязвимый ГПСЧ.

Как пояснил автор исследования ИБ-эксперт Амит Кляйн (Amit Klein), злоумышленник может определить внутреннее состояние ГПСЧ на одном OSI-уровне и использовать эти данные для прогнозирования случайного числового значения на другом OSI-уровне. Таким образом атакующий получает возможность выполнить атаку типа DNS cache poisoning (подмена DNS) на Linux-системах как локально, так и удаленно. Условие заключается в том, что DNS-сервер должен находиться за пределами сети.

По словам специалиста, наиболее уязвимыми к данным атакам являются серверы на Ubuntu - порядка 13,4% web-серверов работают на Ubuntu, 3-5% серверов используют Ubuntu и публичную DNS-службу, удовлетворяя условиям для потенциальной атаки.

Подробнее: <https://www.securitylab.ru/news/515113.php>