

Новая уязвимость предоставляет доступ с правами суперпользователя на системах Linux



Специалисты компании Qualys сообщили о новой уязвимости в ОС Linux, которая позволяет получить права суперпользователя на большинстве дистрибутивов, в частности, Ubuntu, Debian и Fedora.

Проблема (CVE-2021-33909), получившая название Sequoia, содержится в файловой системе Linux и представляет собой уязвимость чтения за пределами буфера (out-of-bounds read). По словам экспертов, проблема связана с некорректной обработкой длины имени файла. С ее помощью непривилегированный локальный пользователь может запустить код с правами суперпользователя.

Экспертам удалось успешно проэксплуатировать проблему на системах с установленными дистрибутивами Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04, Debian 11 и Fedora 34 Workstation. Отмечается, что и другие дистрибутивы Linux, скорее всего, подвержены данной уязвимости.

Эксперты Qualys проинформировали команду разработчиков Red Hat о проблеме в июне нынешнего года. CVE-2021-33909 затрагивает Red Hat Enterprise Linux 8, 7 и 6.

Помимо вышеописанной, Qualys выявила еще одну уязвимость (CVE-2021-33910) в systemd, которая может использоваться для осуществления DoS-атаки. Данная проблема затрагивает Red Hat Enterprise Linux 8.

Источник: <https://www.securitylab.ru/news/522494.php>