Автор: Administrator
20.01.2015 20:08

{jcomments on}

Бреши позволяют злоумышленнику вызвать повреждение памяти и выполнить произвольный код.

Исследователь безопасности Вейсел Хатас (Veysel Hatas) опубликовал подробности о двух уязвимостях в некоторых версиях популярного медиа-плеера VLC. Бреши позволяют злоумышленнику вызвать повреждение памяти и выполнить произвольный код. Одна из уязвимостей связана с нарушением доступа функции предотвращения выполнения данных (DEP), а другая – с доступом к записи данных.

Первая уязвимость, обнаруженная 24 ноября прошлого года, возникает, когда вводимые пользователем данные должным образом не проверяются при обработке специально созданного файла FLV. Подобно первой, вторая брешь возникает, когда вводимые пользователем данные не проверяются корректно при обработке специально созданного файла M2V. Как сообщил Хатас, обе уязвимости могут быть проэксплуатированы «контекстно-зависимым злоумышленником для того, чтобы вызвать повреждение памяти и потенциально выполнить произвольный код».

Бреши, классифицированные как опасные, присутствуют в версиях медиа-плеера VLC 2.1.5 и были протестированы в Windows XP SP3. Поскольку эта платформа больше не поддерживается, а значит, не получит обновлений безопасности, миллионы пользователей по всему миру потенциально подвергаются риску.

Разработчики медиа-плеера VideoLAN получили уведомление о брешах 26 декабря 2014 года, однако исправления до сих пор не выпущены.

Подробнее: http://www.securitylab.ru/news/470064.php