В MS Word обнаружена уязвимость

Автор: Administrator
26.10.2018 19:58

{jcomments on}

В популярном приложении Microsoft Word обнаружили критическую уязвимость, позволяющую удаленно выполнить произвольный код. Проэксплуатировать уязвимость можно, заставив жертву открыть вредоносный документ и кликнуть на встроенное видео.

Проблема связана с тем, как в MS Office обрабатывают видеоматериалы. Злоумышленники могут использовать ее в фишинговых атаках и отправлять жертвам документы со встроенным YouTube-видео (или любым другим online-видео), прикрывая им запущенный в фоновом режиме html- или javascript-код.

Для осуществления атаки злоумышленники должны встроить видео в документ Word, отредактировать XML-файл с именем document.xml и заменить ссылку на видео модифицированной полезной нагрузкой, открывающей менеджер загрузки Internet Explorer со встроенным файлом для выполнения кода.

По словам исследователей, именно в XML-файле и кроется наибольшая угроза. Злоумышленники могут модифицировать параметр embeddedHTML таким образом, чтобы плавающий фрейм видео перенаправлялся на нужный html- или javascript-код.

Официального исправления для уязвимости нет, и единственный способ обезопасить себя от ее эксплуатации – **включить блокировку для файлов со встроенным видео**. Похоже, Microsoft не будет выпускать патч, поскольку ПО работает как положено. «Продукт правильно интерпретирует HTML, как и было задумано, и работает по тому же принципу, что и другие аналогичные продукты», приводит The Register слова старшего директора компании Джеффа Джонса.

Источник: https://www.securitylab.ru/news/496153.php

(function(w, d, n) { w[n] = w[n] || []; w[n].push({ section_id: 263974, place: "advertur_263974", width: 300, height: 250 }); })(window, document, "advertur_sections");