Автор: Administrator
18.11.2015 16:40

{jcomments on}

Уязвимость позволяла получить доступ к личным данным пользователя.

Microsoft устранила уязвимость в функции шифрования диска Bitlocker, которую с легкостью могли проэксплуатировать злоумышленники. По словам ИБ-исследователя Яна Хакена (Ian Haken) из компании Synopsys, реализуемые в Bitlocker меры безопасности можно было обойти с помощью этой бреши.

Хакен рассказал на конференции Black Hat Europe, что персональные компьютеры в доменах больше всех подвержены потенциальным атакам с использованием этой бреши. Злоумышленнику необходимо отключить ПК от сети для того, чтобы доменный сервер был не доступен. В этом случае компьютер на базе Windows использует локальное имя пользователя и пароль, сохраненный в кеше.

ИБ-исследователь обнаружил способ получения доступа к паролю в кеше и его изменению. Таким образом, злоумышленник может обойти функцию шифрования всего диска. Эксперт объяснил, что при создании поддельного доменного сервера с таким же именем, злоумышленнику остается только создать учетную запись с паролем, созданным пользователем ранее. Это действие провоцирует изменение пароля согласно правилам безопасности. Злоумышленник может изменить пароль и зайти в систему, используя пароль, сохраненный в кеше.

После входа в систему хакер получает доступ ко всей информации пользователя, в том числе к сообщениям в электронной почте, сохраненным паролям, кешированным учетным данным и пр. «Если пользователь является локальным администратором, злоумышленник даже может сбросить ключ шифрования Bitlocker из памяти ядра», - отметил Хакен.

В настоящее время нет свидетельств эксплуатации уязвимости злоумышленниками.

Источник: www.securitylab.ru