Автор: Administrator
14.08.2015 16:20

{jcomments on}

Атакующий может повысить свои привилегии и выполнить вредоносный код на целевой системе.

Microsoft в рамках «вторника обновлений» предупредила пользователей о том, что злоумышленники с помощью USB-устройств эксплуатируют уязвимость в продукте компании, позволяющую выполнить вредоносный код. Брешь затрагивает все поддерживаемые версии ОС Windows.

Уязвимость существует из-за того, что компонент Mount Manager некорректно обрабатывает символические ссылки. Локальный злоумышленник может повысить свои привилегии и выполнить код. Для того чтобы проэксплуатировать уязвимость, атакующему необходимо подключить вредоносное USB-устройство к целевой системе.

Данная брешь CVE-2015-1769 очень напоминает уязвимость .LNK, которую в прошлом эксплуатировали создатели Stuxnet, отмечает ИБ-исследователь Пьерлуиджи Паганини. Единственное различие между брешами заключается в том, что эксплуатировать первую можно только локально с помощью вредоносных USB-устройств, а вторую - удаленно.

Компания Microsoft полагает, что данная брешь эксплуатируется злоумышленниками в кибератаках на пользователей продуктов компании. Устранить уязвимость можно, установив обновления с сайта производителя.

Источник: http://www.securitylab.ru/news/474219.php