Автор: Administrator
07.01.2018 16:50

{jcomments on}


3 января 2018 года стало известно об уязвимостях, затрагивающих процессоры Intel, ARM64 и частично AMD. Как сообщают исследователи из команды Google Project Zero, Meltdown позволяет повысить привилегии на системе и из пространства пользователя прочитать содержимое любой области памяти, в том числе память ядра и чужой памяти в системах паравиртуализации (кроме режима HVM) и контейнерной изоляции. Проэксплуатировать уязвимость может любой пользователь, у которого есть возможность выполнить код на системе. Проблема затрагивает практически все версии процессоров Intel, начиная с 1995 года (исключение составляют Intel Itanium и Intel Atom до 2013 года), и ARM64 (Cortex-A15/A57/A72/A75). Как и Meltdown, Spectre позволяет повысить привилегии и получить данные приложения, запущенного другим пользователем. Тем не менее, в отличие от Meltdown, прочитать память ядра с помощью Spectre нельзя. Воспользоваться уязвимостью может любой, у кого есть возможность выполнить код на системе. Проблема затрагивает процессоры Intel, AMD (только при включенном eBPF в ядре) и ARM64 (Cortex-R7/R8, Cortex-A8/A9/A15/A17/A57/A72/A73/A75). Подробнее: www.securitylab.ru

Разработчики компании Microsoft выпустили внеочередные обновления безопасности, исправляющие опасные уязвимости Meltdown и Spectre.

Для операционных систем Windows 7 и Windows Server 2008 R2 доступно обновление KB4056897

.

Для операционных систем Windows 8.1 и Windows Server 2012 R2 доступно обновление KB4056898

.

Для операционных систем Windows 10 и Windows Server 2016 доступны обновления: KB 4056888
(версия 1511),
KB4056891
(версия 1703),
KB4056568
).