One Solution. One Company.

Отчет по безопасности (SN-20180101)

Уязвимости Meltdown и Spectre

Версия 1.0

(26 Января 2018)

Содержание

1 Обзор

3 января 2018 года, были обнаружены уязвимости в безопасности в большинстве современных процессоров под названием Meltdown и Spectre.

В этом документе содержится краткое описание уязвимостей Meltdown и Spectre, а также влияние этих атак на продукты IDIS.

2 Что такое Meltdown и Spectre?

Аппаратные уязвимости, называемые Meltdown и Spectre, позволяют красть данные, которые в настоящее время обрабатываются на компьютере. В то время как программам, как правило, не разрешено считывать данные из других программ, вредоносная программа может использовать Meltdown и Spectre для сбора данных, хранящихся в памяти других запущенных программ. Это могут быть ваши пароли, хранящиеся в диспетчере паролей или в браузере, ваши личные фотографии, электронные письма, мгновенные сообщения и даже критически важные для бизнеса документы [1].

Злоумышленники могли воспользоваться спекулятивным исполнением, чтобы читать системную память, которая должна была быть недоступна. Например, неавторизованная сторона может считывать конфиденциальную информацию в памяти системы, такую как пароли, ключи шифрования или конфиденциальную информацию, открытую в приложениях [2].

Эти уязвимости затрагивают многие процессоры, в том числе AMD, ARM и Intel, а также устройства и операционные системы, работающие на них [2].

(1) Meltdown

- Variant 3 : CVE-2017-5754 (Rogue data cache load)

Доступ к памяти, управляемой ОС при запуске вредоносного приложения [6].

Meltdown использует оптимизацию производительности процессора, называемую «исполнение вне порядка», и обеспечивает доступ к произвольной памяти ядра в пространстве пользователя. Это означает, что злоумышленники могут получить доступ к различным данным, связанным с безопасностью, существующей в системе.

(2) Spectre

- Variant 1 : CVE-2017-5753 (Bounds check bypass)

Использует существующий код с доступом к секретам, заставляя его спекулятивно выполнять операции памяти с аргументами вне диапазона [6].

- Variant 2 : CVE-2017-5715 (Branch target injection)

Вредоносный код узурпирует свойства функций предсказания ветвления процессора для спекулятивного выполнения команд [6].

Spectre - уязвимость, которая использует повышение нагрузки на ЦП, известное как спекулятивное исполнение. Предоставляя доступ к конфиденциальным данным в памяти ядра, эта уязвимость позволяет злоумышленнику с низким уровнем привилегий получать доступ не только к области ядра, для которой требуются высокие привилегии, но также к области процессов других пользователей.

3 Воздействие Meltdown и Spectre на продукты IDIS

3.1 Standalone: NVR, DVR и IP-видекамеры

IDIS используют центральные процессоры ARM, для которых уязвимости Meltdown до сих пор не были затронуты.

IDIS регистраторы и IP-видеокамеры с кодеком H.265 и разрешением 8МП и выше могут быть уязвимы для Spectre Variant 1 и Variant 2.

Тем не менее, очень сложно атаковать эти продукты IDIS с использованием Spectre по следующим причинам:

(1) IDIS не предоставляет возможность загрузки стороннего программного обеспечения и не имеет механизмов для загрузки и выполнения произвольных программ для пользователей [7].

(2) IDIS шифрует информацию, необходимую для защиты, например информацию пользователя и пароль, чтобы предотвратить использование пользователями неавторизованных пользователей.

(3) Spectre может использовать javascript, работающего в веб-браузере. Но продукты IDIS не предоставляют веб-браузер и не позволяют использовать этот подход.

В дальнейшем, если будет предоставлены исправления от производителей ЦП или ОС, они могут быть применены к некоторым из последних продуктов IDIS, таких как IDIS NVR, HD-TVI на базе H.265 и IP-видеокамерам после оценки того, насколько изменения существенно повлияют на производительность системы.

3.2 NVR на базе ПК : IR-1000, IR-100

NVR на базе ПК используют процессоры Intel и в настоящее время имеют как уязвимости Meltdown, так и Spectre. Таким образом, риск утечки данных из NVR на базе ПК из-за этих уязвимостей выше, чем у автономных продуктов.

Тем не менее, NVR на ПК работают на Windows Embedded OS 8, которая удаляет ненужные службы Windows и порты доступа к сети и относительно устойчива к введению вредоносного кода через сеть по сравнению с другими ОС Windows, используемыми для серверов или рабочих станций.

В дальнейшем, если будет предоставлены исправления от производителей ЦП или ОС, они могут быть применены после оценки того, насколько изменения существенно повлияют на производительность системы.

3.3 Программное обеспечение: IDIS Center и IDIS Solution Suite

На программное обеспечение IDIS эти уязвимости не влияют и никаких изменений не предполагается.

Большинство программных продуктов IDIS работают на ОС Windows и процессорах Intel, AMD или ARM. Таким образом, пользователь должен рассмотреть возможность установки исправлений, предоставленных производителем процессоров и ОС после проверки модели процессора и версии ОС Windows на ПК, на котором установлено программное обеспечение IDIS.

Кроме того, следует отметить, что установка патча может вызвать заметное ухудшение производительности в зависимости от типа процессора и ОС [9].

Контакты

Информация может быть обновлена в этом документе. Пожалуйста, обратитесь в IDIS по электронной почте support@idisglobal.ru, если у вас есть какие-либо вопросы или проблемы, связанные с этой проблемой

Источники

[1] https://meltdownattack.com/

[2] https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

[3] https://meltdownattack.com/meltdown.pdf

[4] https://spectreattack.com/spectre.pdf

[5] www.cve.mitre.org/

[6] https://developer.arm.com/support/security-update/frequently-asked-questions

[7] https://ipvm.com/reports/intel-flaw

[8] https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)

[9] https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Blog-Benchmark-Table.pdf

Историй версий

Версия	Автор	Дана	Комментарий
1.0	Daniel Lee	26 Января 2018	Начальная публикация