Найдены параметры управления:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\FeatureSettingsOverride]
“Spectre_Mitigation_ControlFlags”=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\FeatureSettingsOverride]
“L1TF_Mitigation_ControlFlags”=dword:00000000

- это сомнительная инфа, я не нашел их в ядре. Выполни поиск уточнить достоверная ли инфа.

Прочитано 14 веб-страниц

Информация, которую вы нашли, **в целом достоверна**, но в ней есть важная неточность в названии параметра. Это не `Spectre_Mitigation_ControlFlags` и не `L1TF_Mitigation_ControlFlags`, а стандартные ключи реестра `FeatureSettingsOverride` и `FeatureSettingsOverrideMask`.

Эти параметры действительно являются официальным механизмом, который Microsoft предоставляет для управления смягчением последствий уязвимостей, связанных со спекулятивным исполнением, таких как Spectre, Meltdown, L1TF и другие [1] [4] [10].

🔍 Что подтверждает поиск

Множество источников, включая официальную документацию Microsoft, указывают на эти ключи:

- **Официальный путь в реестре**:

```
text

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
```

- **Имена параметров**: FeatureSettingsOverride (тип REG_DWORD) и FeatureSettingsOverrideMask (тип REG_DWORD) [1] [2] [3].

Их функциональность подтверждается множеством источников, включая статьи Microsoft, обсуждения на форумах и рекомендации по управлению производительностью [1] [2] [3]. Ключи могут отсутствовать в реестре по умолчанию — их нужно создавать вручную [3] [7] [9].

🤔 Почему вы не нашли их в ядре?

Вероятно, вы искали по неверным именам (Spectre_Mitigation_ControlFlags и L1TF_Mitigation_ControlFlags). В ядре Windows они не встречаются, потому что это неправильные названия. Официальные имена — FeatureSettingsOverride и FeatureSettingsOverrideMask, которые используются как общий механизм управления для целого набора уязвимостей.

⚙️ Как это работает (кратко)

- FeatureSettingsOverrideMask: Это битовая маска, которая определяет, какие биты в FeatureSettingsOverride будут применены. Обычно для активации изменений ей устанавливают значение 3 [1] [3] [5]. Это означает, что будут учитываться младшие два бита FeatureSettingsOverride.
- FeatureSettingsOverride: Это битовое поле, где каждый бит управляет конкретной защитой. Основные значения:
  - 0: **Включить** защиты для Spectre Variant 2 (CVE-2017-5715) и Meltdown (CVE-2017-5754) [7] [12].
  - 1: **Отключить** защиту для Spectre Variant 2 [7].
  - 2: **Отключить** защиту для Meltdown [7].
  - 3: **Отключить** защиты для Spectre Variant 2 и Meltdown [1] [2] [5].

Со временем этот механизм был расширен для управления и более новыми уязвимостями, такими как L1TF (Foreshadow) [2] [4] [8] или Downfall (GDS) [1] [13] [14].

💎 Итог

Информация о существовании ключей реестра для управления патчами Spectre и L1TF является достоверной. Ваша находка содержит правильный путь в реестре, но ошибочные имена параметров. Правильные названия: FeatureSettingsOverride и FeatureSettingsOverrideMask.

14 веб-страниц

Найди точные параметры, описание бит, дефейны.

Прочитано 13 веб-страниц

Вы нашли правильный путь в реестре, но точное описание параметров и их значений немного сложнее.

Точные параметры реестра

- **Путь в реестре:**

  text

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

- **Имена значений:**
  - FeatureSettingsOverride (тип REG_DWORD)
  - FeatureSettingsOverrideMask (тип REG_DWORD)

Описание бит и значений

FeatureSettingsOverride — это битовое поле. Важнейший нюанс: **бит, равный 0, включает защиту, а бит, равный 1, — отключает** 1 3 12.

- **Бит 0 (значение 1):** Управляет защитой от уязвимости **Spectre Variant 2 (CVE-2017-5715).** 0 — защита включена, 1 — защита отключена 1 12.
- **Бит 1 (значение 2):** Управляет защитой от уязвимости **Meltdown (CVE-2017-5754).** 0 — защита включена, 1 — защита отключена 1 12.

Параметр FeatureSettingsOverrideMask является битовой маской, которая определяет

Параметр `FeatureSettingsOverrideMask` является битовой маской, которая определяет, какие биты из `FeatureSettingsOverride` будут применены [1] [12]. Для включения/отключения управления первыми двумя битами, этому параметру обычно задают значение `3` (двоичное `11`) [2] [6] [7].

Распространенные комбинации значений

Основное действие	FeatureSettingsOverride	FeatureSettingsOverrideMask	Примечание
Включить защиты (по умолчанию для клиентских Windows)	0	3	Оба бита установлены в `0`, что включает защиты для Spectre и Meltdown [3] [6].
Отключить защиты	3	3	Оба бита установлены в `1`, что отключает защиты для Spectre и Meltdown [2] [9].
Включить Spectre, отключить Meltdown	2	3	Бит 0 = 0 (Spectre включен), Бит 1 = 1 (Meltdown отключен) [1] [12].

Дополнительные биты для других уязвимостей

Обратите внимание, что эти два бита управляют только самыми первыми и известными уязвимостями Spectre и Meltdown. Позже Microsoft расширила этот механизм для управления и другими уязвимостями. Значения для них могут быть более сложными [3] [5] [7].

- **CVE-2018-3639 (Speculative Store Bypass)**: Для включения защиты вместе с Spectre и Meltdown используется значение `8` (0x8) для `FeatureSettingsOverride` [5] [7] [10].

- **AMD процессоры**: Для AMD процессоров могут использоваться другие комбинации, например, 72 (0x48) 3 5 8 .
- **Intel BHI (CVE-2022-0001)**: Для Intel процессоров могут использоваться значения с установленными старшими битами, например, 8388680 (0x800048) 8 .
- **Downfall (CVE-2022-40982)**: Для его отключения используется старший бит со значением 0x2000000 (hex) 9 13 .

Рекомендация: Назначать произвольное число для FeatureSettingsOverride без понимания всех установленных битов небезопасно, так как это может случайно отключить защиту от других критических уязвимостей. Всегда обращайтесь к актуальной документации Microsoft для вашей конкретной версии Windows.

13 веб-страниц

Продолжить с DeepSeek