



Группа инженеров опубликовала в сети код для неустранимого взлома USB



Вадим
Елистратов
[@great_laziness](#)

3 ОКТЯБРЯ, 11:37

11 222 66

Инженеры Адам Коудилл (Adam Caudill) и Брэндон Уилсон (Brandon Wilson) опубликовали на [GitHub](#) инструкцию по взлому порта USB с помощью неустранимой уязвимости, о существовании которой [было объявлено](#) в конце июля. Об этом сообщает [Wired](#).



В конце июля исследователи в области компьютерной безопасности Карстен Нол и Джейкоб Лелл заявили, что в результате реверс-инжиниринга прошивки, отвечающей за коммуникационные функции порта USB, им удалось найти в нём неустранимую уязвимость.

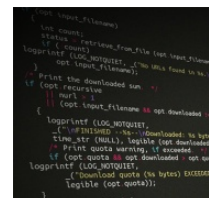
Эта «дыра» позволила инженерам написать код под названием BadUSB, который позволяет заражать компьютеры с помощью устройств, у которых даже нет собственной памяти: вирус хранится непосредственно в чипе-контроллере, и поэтому не может быть обнаружен любыми стандартными средствами.

Тогда Нол и Лелл отказались публиковать свою находку в сети, чтобы дать индустрии время разобраться с проблемой, однако спустя два месяца это решение приняли за них. В рамках конференции DerbyCon инженеры Адам Коудилл и Брэндон Уилсон заявили, что им удалось повторить BadUSB, но они убеждены, что только публикация этого кода в сети может заставить крупные корпорации задуматься.



Если подобное могут сделать только люди с большим бюджетом, производители пальца о палец не ударят. Мы должны доказать миру, что на практике подобное может

Читайте также материалы по теме



Баг в командной оболочке Bash позволял хакерам годами контролировать компьютеры на Linux и Mac OS

25 Сентября

14 772 64

сделать кто угодно.

— Адам Коудилл

Поскольку проблема BadUSB кроется в самой сути стандарта USB, в текущих его версиях (2.0 и 3.0) её устранить нельзя. Для этого нужна новая версия USB с дополнительным слоем защиты.

“Люди смотрят на эти штуки [флешки] и не видят в них ничего кроме хранилищ данных. Они не понимают, что держат в руках перепрограммируемый компьютер.

— Адам Коудилл

BadUSB может быть использован для захвата управления PC, скрытого изменения файлов пользователя и перенаправления интернет-трафика. Более того, после того, как флешка заразила компьютер, он может заразить и другое USB-устройство, тем самым запустив эпидемию.

2014 год уже по праву можно считать годом глобальных уязвимостей, подобных этой. Весной серьёзную «дыру» [обнаружили](#) в стандарте шифрования данных OpenSSL, из-за чего многим крупным сайтам пришлось сбросить пароли своих пользователей, а в конце сентября — в популярной среди пользователей Linux и Mac командной оболочке [Bash](#). На полное устранение этих проблем могут уйти годы.

Брэндон Уилсон

BadUSB

Адам Коудилл

взлом USB

Карстен Нол

Джейкоб Лелл

Показывать сверху

старые

новые

популярные

Lx Lx11 часов назад

Так бежали в будущем, что попадаем в прошлое

0

Я молодец10 часов назад

Это касается и переносных жёстких дисков, полагаю?

0

Влад Колосов10 часов назад

Любое USB устройство: мышки, клавиатуры, портативные HDD, принтеры и так далее

5

Настя Иванова10 часов назад

Решение проблемы

0

Настя Иванова10 часов назад

53

Игорь Николаев9 часов назад

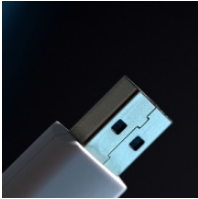
Думаю, речь идёт, всё же, о флешках. Откуда чип в кабеле мышки? Зачем он там? Просто провод с контактами. Не надо преувеличивать. У страха глаза велики?)

-4

Ilya Makeev9 часов назад

у страха глаза

9



Компьютеры научились заражать с помощью уязвимости в стандарте USB

31 Июля


5 30734




Баг в пакете OpenSSL поставил под угрозу безопасность сотен тысяч сайтов

9 Апреля


11 05223

- 


Ilya Makeev 9 часов назад
А вообще не стоит говорить о том, чего не знаешь, за умного...)

0
- 


Игорь Николаев 9 часов назад
Я смотрю, ты больно умный) Нет там никакого чипа, специально кабель зарядки расковырял) Ты правда думаешь, что для передачи данных или электричества всенепрерменно нужен чип?

0
- 


Slava Zlodeev 4 часа назад
В любом usb устройстве есть чип, который и формирует выходной сигнал, вот например мышка.

1
- 

Віталій Кузишин 4 часа назад
Я даже авторизовался, чтобы заминусовать то, что вы здесь написали. Жаль не удалось.


1
- 

Вячеслав Чиликанов 5 часов назад
Ну если мышка-это провод с контактами, то флешка-просто контакты))))))


0
- 

Илья Сазонов 10 часов назад
Вообще всего, что использует USB. Даже в data-кабель, по идее, можно всунуть этот чип.


0

- 


Max Sha 10 часов назад
Пока неясно, как атаковать компьютер. Атакой драйвера?

0
- 

Илья Сазонов 10 часов назад
Кож же на гитхабе лежит, посмотрите.

1
- 


Илья Сазонов 10 часов назад
*Код

0
- 

Max Sha 9 часов назад
Очевидно, посмотрел.
Там лежит код инъекции кода в прошивку.

Чтобы с его помощью заразить компьютер, нужно (а) USB-устройство вполне определённого производителя и (б) написать атаку на все возможные драйвера для этого устройства и ОС). И даже это не всегда будет работать.

Возможно, я что-то упускаю, потому и задал вопрос.

2
- 

ValdikSS 9 часов назад
Да это, по большому счету, слишком громкий заголовок, всего-то. Суть в том, что некоторые контроллеры флешек слишком умные, и вся их логика зависит от прошивки. Эти ребята перепрошивают такие контроллеры, чтобы они представлялись дополнительно как NDIS-устройство, например (сетевой адаптер), и из-за того, что некоторые ОС автоматически попытаются подключить такой адаптер и (если есть default route) перенести весь трафик на него, это

5

(если есть белый кабель) перенести весь трафик на него, это довольно опасно. Но это заметно, что появился еще один адаптер.

**Влад Колосов**

10 часов назад

Любое USB устройство: мышки, клавиатуры, портативные HDD, принтеры и так далее

0

**Влад Колосов**
Промахнулся

10 часов назад

0

**Насущные Проблемы**

10 часов назад

Шутка про презерватив на разъеме.

2

**Emil Sharifullin**

9 часов назад

Таки не шутка <http://habrahabr.ru/post/194316/>
Только именно эта штука не выход в данном случае

0

**Сергей Пелевин**

10 часов назад

Дружище, одолжи клавишу на пол часика, мне у себя кой-чо проверить, сразу верну
Ой, у тебя она блютуз? Не, не надо, забей

13

**Сергей Гладышев**

10 часов назад

проводная так-то не лучше. там тоже есть юсб разъем.
нужна PS/2

4

**Настя Иванова**

10 часов назад

Как-то так

8

**Я молодец**

10 часов назад

скрытая реклама маков

-15

**Александр Евсюков**

10 часов назад

Ну, да. Мак ведь флешек не использует)))

19

**Nick Yasnov**

9 часов назад

Ну я лично флешкой пользуюсь раз в год. Кому они нужны-то ещё? Так что мне словить такой вирус будет проблематично)

0

**Stanislav Moroz**

9 часов назад

А других USB-устройств у тебя нет?












0


**Nick Yasnov**

9 часов назад


У меня есть мышь и клавиатура. Теперь думаем, где я могу подцепить зловред, который мне перенесётся через USB-контроллер. Подсказка: я не хожу по чужим домам с мышкой и клавиатурой.


0

-  **Emil Sharifullin** 9 часов назад
И даже телефон к чужой зарядке не подключаешь? 0
-  **Nick Yasnov** 9 часов назад
Нет. Тем более, у кого сейчас можно найти зарядку для 30-pin? 0
-  **Stanislav Moroz** 9 часов назад
У меня две. 0
-  **Nick Yasnov** 8 часов назад
Держись-ка подальше от моего телефона. 3
-  **Stanislav Moroz** 6 часов назад
Я то же самое своей девушке говорю. 2
-  **Lx Lx** 8 часов назад
Олдфаг брать тоже мне 0
-  **Nick Yasnov** 8 часов назад
Нищеврод(0
-  **Stanislav Moroz** 9 часов назад
Через чужой провод для айфона? 0
-  **Юрий Тетюриков** 8 часов назад
Пришёл к тебе знакомый и говорит: "ой, слушай, я тут на флешке принёс %то-что-тебя-заинтересует%, глянем?" 0
-  **Nick Yasnov** 7 часов назад
В моём городе уже слышали про дробокс, спасибо. 0
-  **Я молодец** 10 часов назад
зря написал 13

 **Ivan Kharitonov** 10 часов назад
Вот это поворот! 0

 **Alex D** 10 часов назад
Вот оно как... -12

 **V.Prosh** 10 часов назад
Интернет и компьютеры это вообще опасно 1

 **Snow Dimon** 8 часов назад
ЗАПРЕТИТЬ!!!!!!
ЗАПРЕТИТЬ ЗАПРЕТИТЬ!!!!!! 3

НАВЕСТИ ПОРЯДОК!!!

**Kostya Osmolovsky**

10 часов назад

Uncurable
Security
Breach

3

**Evgeny Gladkikh**

10 часов назад

Вангую что так и залили Стакнет года назад.

0

**Хижина дяди Кермана**

8 часов назад

+1, на похожем принципе небось и распространялся.

0

Теперь, даже на далеких от высоких технологий производствах, запрещают использовать незареганные в системе флешки.

**Артур Кимзянов**

10 часов назад

Тем временем, какой-нибудь депутат уже пишет закон о запрете USB)

8

**Кот и в Твиттере Кот**

10 часов назад

та не, им еще о USB не доложили.

0

**Влад Ярославлев**

7 часов назад

В пенсионном фонде и прочих налоговых до сих пор на дискетах всё

0

**Илья Гераськин**

10 часов назад

Таким образом старый киношный трюк, где герой вставляет в комп флешку и тем самым взламывает систему уже не будет смешным.

12

**Кот и в Твиттере Кот**

10 часов назад

Ну подводные лодки к нам тоже пришли из искусства.

0

**Влад Маришин**

9 часов назад

Через месяц какой появятся противозачаточные от этого недуга. Вот и стимул к работе.

0

**mofovik**

9 часов назад

Мы хотим избавить мир от алкоголизма, вот вам рецепт нашего самогона. Все логично. Если есть угроза - давайте сделаем ее опасностью. Какие молодцы Адам и Брендон

0

**Alexey Gukov**

9 часов назад

Переход на облачные хранилища данных решит, конечно, пару проблем.
Вот только что делать со всеми другими штуками, использующими usb?

0

**Роман Хуторянский**

4 часа назад

мышь и клавиша как один раз всунул. так и не свю их никак

0

больше, они верные у меня))
остается только usb как способ зарядить телефон, ибо
передача данных через usb также давно прошлый век

Alexey 3 минуты назад

А какая альтернатива проводу? Заливаю так сериалы на телефон. Пробовал вай фай подключение, но пара серий по гигабайту передается вечность, а по проводу за несколько минут закачивается...

Alex D 9 часов назад

А сколько еще таких моментов в наших устройствах о которых мы еще даже и не знаем. Расслабьтесь.

moskov_sky 7 часов назад

Где фото голых USB-портов??

Vadim Smorodov 6 часов назад

Ребят, как и в прошлый раз, чуть меньше желтушности

Владислав Фаустов 5 часов назад

"Более того, после того, как флешка"...

Nikita Golodenko РЕЗИДЕНТ 5 часов назад

«А вот теперь бойся, Петяка...»

Nihsamor Namreg 5 часов назад

Ну теперь-то FireWire будет шикавать.

Алексей Кузнецов 4 часа назад

Хм, а что, все USB-устройства (точнее даже контроллеры!) являются перепрограммируемыми?

Vadim Semenov 4 часа назад

Оставить комментарий

TWITTER

ВКОНТАКТЕ

FACEBOOK

Авторизуйтесь, чтобы
проголосовать или
оставить комментарий.

Нашли опечатку? Выделите фрагмент и отправьте нажатием Ctrl+Enter.

Лучшее за [неделю](#) / [месяц](#) / [год](#)



Где взять качественные обои для нового смартфона

Статья / 2 Октября

9 486 48



8 главных цитат из интервью Галины Тимченко про новое интернет-СМИ Meduza

Статья / 1 Октября

6 155 39



Как телефонам BlackBerry удалось стать символом корпоративной культуры

Статья / 2 Октября

10 082 81



Шестеро британцев согласились обменять своих первенцев на бесплатный Wi-Fi

Новость / 1 Октября
8 231 42

TJOURNAL

editors@tjournal.ru

[Карта сайта](#)

[Партнер Рамблера](#)

[О проекте](#)

[Команда](#)

[Реклама](#)

