CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 12.05.2020 г.

Съдържание

Недостатъци в сигурността на Thunderbolt засягат системите преди 2019 година

11 май 2020 г.

Нападателите, които получават физически достъп до Windows, Linux или macOS устройства, могат да получат достъп и да откраднат данни от техните твърди дискове, като използват 7 уязвимости, открити в хардуерния интерфейс на Intel Thunderbolt и известни като Thunderspy.

Thunderbolt е хардуерен интерфейс, проектиран от Intel и Apple с цел да помогне свързването на външни периферни устройства, които се нуждаят от високоскоростни връзки (RAID масиви, мрежов интерфейс, устройства за заснемане на видео и други) към компютър.

Новата атака е предназначена да наруши сигурността на Thunderbolt, като прави възможно нападателите да откраднат информация от всяко уязвимо устройство с активиран Thunderbolt.

Системите преди 2019 г. са уязвими

Въпреки че от Intel твърдят, че Windows, Linux и macOS са внедрили защитата на Kernel Direct Memory Access (DMA) за смекчаване на подобни атаки, защитата не смекчава всички възможни сценарии за атака и е достъпна само на съвместими системи, доставяни от 2019 г. и по-късно. Следователно всички системи, пуснати преди 2019 г., и по-новите системи, които не доставят Kernel DMA Protection, са напълно уязвими за Thunderspy.

За потребители на Linux и Windows всички системи, закупени преди 2019 г., са уязвими към Thunderspy атаки, докато устройствата, закупени по време и след 2019 г., може да се предлагат с поддръжка на Kernel DMA Protection, която предпазва от атаки с директен достъп до паметта.

По същия начин, Macs от 2011 г. и по-стари, с изключение на Retina MacBooks, са засегнати от Thunderspy, тъй като всички те предоставят на потребителите Thunderbolt свързаност.

Thunderspy е кражба, което означава, че не могат да се намерят следи от атаката. Атаката не изисква участието на потребител, т.е. няма фишинг връзка или злонамерен хардуер, който нападателят ви подмамва да използвате.

Thunderspy работи, дори ако следвате най-добрите практики за защита, като заключите или спрете компютъра си, когато напускате за кратко, и ако системният ви администратор е настроил устройството със Secure Boot, силна парола за BIOS и акаунт за операционна система и е активирал пълно криптиране на диска.

Специалист по сигурността е открил 7 уязвимости в дизайна на Intel и е разработил 9 реалистични сценария как те могат да бъдат експлоатирани от някого, за да получи достъп до вашата система, въпреки защитите, които Intel е създал.

Досега е установено, че тези 7 проблема със сигурността влияят на Thunderbolt 1 и 2 (над Mini DisplayPort) и Thunderbolt 3 (над USB-C):

- Неадекватни схеми за проверка на фърмуера
- Слаба схема за удостоверяване на устройствата
- Използване на неавтентифицирани метаданни на устройството
- Downgrade атаки, използващи обратна съвместимост
- Използване на неоторизирани конфигурации на контролера
- Недостатъци на SPI флаш интерфейса
- Липса на защита от Thunderbolt на Boot Camp

Intel потвърди, че уязвимостите на Thunderspy са валидни, но няма да бъдат смекчени чрез издаване на пачове на вече продадени и известни като уязвими устройства, тъй като те ще изискват преработка.

Intel увери, че ще включва допълнителна хардуерна защита за бъдещи системи, които идват с поддръжка на технологията Thunderbolt.

Ето какво още Intel потвърди относно уязвимостите:

- И трите версии на Thunderbolt са засегнати от уязвимостите на Thunderspy.
- Само системи, доставящи защита на Kernel DMA, смекчават някои, не всички уязвимости на Thunderspy.
- Само системи, които се доставят от 2019 г., идват с Kernel DMA Protection

- Освен защитата на Kernel DMA, Intel няма да предоставя никакви смекчаващи мерки за справяне с уязвимостите на Thunderspy. Следователно Intel няма да присвоява никакви CVE на уязвимостите на Thunderspy или да пуска каквито и да било съвети за обществена сигурност, за да информира широката общественост.

Докато Intel не прилага хардуерни защити на Thunderspy, можете да следвате тези препоръки, за да защитите данните си или да деактивирате Thunderbolt контролера в UEFI (BIOS).

Специалист по киберсигурност разработи и Spycheck, инструмент, който помага на потребителите да проверяват дали техните компютри са засегнати от уязвимостите на Thunderspy и предоставя препоръки как да защитите системите си от атаки.

Миналата година екип от изследователи разкриха друг набор от уязвимости в защитата - наречен Thunderclap - изискващи физически достъп и засягащи съвременни компютри, поддържащи Thunderbolt, които работят под Windows, macOS, Linux или FreeBSD.

Недостатъците на Thunderclap могат да бъдат използвани за стартиране на произволен код, използвайки възможно най-високото ниво на привилегия в системата за достъп или кражба на „пароли, банкови входни данни, ключове за криптиране, частни файлове, сърфиране“, както и други чувствителни данни, налични на уязвимата машина.

За повече информация:

https://www.bleepingcomputer.com/news/security/new-thunderbolt-security-flaws-affect-systems-shipped-before-2019/

Office 365 позволява на обикновените потребители да отменят криптирани съобщения

11 май 2020

Microsoft работи върху разширяването на възможностите за отмяна на криптирани имейл съобщения, изпратени с помощта на услугата за шифроване на

съобщения на Office 365 (OME) на редовни потребители, като част от по-големи усилия за предотвратяване на изтичане на данни и кражба на корпоративни данни.

OME е изграден върху Microsoft Azure Rights Management (Azure RMS) и съчетава управление на права с възможности за криптиране на имейли. Позволява на клиентите на Office 365 да изпращат и получават криптирани имейли с помощта на Outlook.com, Yahoo !, Gmail и няколко други имейл услуги с поддръжка за криптиране, оторизация и политики за идентичност.

Като част от Advanced Message Encryption за Office 365, Microsoft разширяват възможностите за отмяна на имейл до крайния потребител. Преди това трябваше да сте администратор, за да оттеглите вече изпратено съобщение; с тази актуализация крайните потребители ще имат и тази възможност.

Тази нова възможност ще бъде достъпна само за потребители на Office 365 с поддръжка за Advanced Message Encryption като Microsoft 365 Enterprise E5, Office 365 E5, Microsoft 365 E5 (Nonprofit Staff Pricing), Office 365 Enterprise E5 (Nonprofit Staff Pricing), and Office 365 Education A5.

Въпреки че Microsoft не обяснява какво ще се случи с отменените криптирани съобщения, когато администраторите отменят такива имейли, получателите получават „Съобщението е отменено от изпращача“ при опит за достъп до шифрованите имейли чрез Портала за шифроване на съобщения в Office 365.

Екипът на Microsoft Exchange планира да въведе това ново разширение на възможностите на OME през последното тримесечие на 2020 г. и то ще бъде общодостъпно в световен мащаб за много потребители.

Като част от по-големите си усилия за спиране на кражбите на корпоративни данни, Microsoft също планира да деактивира препращането по електронна поща за Office 365 до външни получатели по подразбиране, стартирайки от четвъртото тримесечие на 2020 г.

Microsoft работи и за подобряване на начина, по който имейлите, изпратени чрез OME услугата, се разпознават от пощенските сървъри, така че да е по-малко вероятно да бъдат изпратени в папката Trash, след като бъдат маркирани като спам.

Тук можете да намерите бърз преглед на възможностите за шифроване на съобщения в Office 365 с инструкции за изпращане на защитени имейли до почти всеки в и извън вашата организация.

За повече информация:

https://www.bleepingcomputer.com/news/microsoft/office-365-to-let-regular-users-revoke-encrypted-messages/