

Мониторинг на актуалните киберновини – към 01.06.2020 г.



Съдържание

Подготовка за следващите инциденти в киберсигурността	2
Ето какви са новите функции за защита в Windows 10 2004.....	4
VMware поправя Fusion уязвимост, въведена с предишен пач	8

Екип за реагиране при инциденти в компютърната сигурност

Подготовка за следващите инциденти в киберсигурността

29 май 2020

Агенцията за киберсигурност на ЕС ENISA публикува нов доклад и хранилище към него, съдържащо мерки и източници на информация за проактивно откриване на инциденти.

Към април 2020 г. повече от 500 европейски екипа за реакция при инциденти са включени в мрежата на Екипите за реагиране при инциденти в компютърната сигурност (CSIRT) - [интерактивна карта](#) на екипите по държави . Те работят ежедневно за подобряване предотвратяването, откриването и анализа на кибер заплахи и инциденти.

Както е предвидено в NIS директивата и в Закона за киберсигурност на ЕС, на ENISA е възложена отговорността да съдейства на CSIRT мрежата и на държавите-членки за подобряване на предотвратяването, откриването и способността да реагират на кибер заплахи и инциденти, като им предоставя знания и опит. В този контекст ENISA стартира проект с цел да подобри активното откриване на инциденти, свързани със сигурността на мрежата в ЕС чрез:

- Предоставяне на списък на наличните мерки и източници на информация;
- Определяне на добри практики;
- Препоръчване на възможни области за развитие.

В тази връзка проактивното откриване на инциденти се определя като процес на откриване на злонамерена дейност чрез вътрешни инструменти за мониторинг или чрез външни организации, които публикуват информация за открити инциденти, преди засегнатите участници да са станали наясно с проблема.

ENISA публикува първата версия на такова проучване, озаглавено [„Проактивно откриване на инциденти“](#) през 2011 г.

Текущата разработка надгражда и разширява предишната. Тя има за цел да предостави пълен списък на всички налични методи, инструменти, дейности и източници на информация за проактивно откриване на инциденти. Подобни инструменти вече се използват или биха могли да се използват от екипите за реагиране при инциденти в Европа.

Екип за реагиране при инциденти в компютърната сигурност

Проучването идентифицира развитието на проактивното откриване на инциденти в ЕС в периода 2011 г. - 2019 г. Освен това изследва нови области, които биха могли да помогнат за подобряване на оперативното сътрудничество и обмена на информация. Целта е да се помогне както на новите екипи, които започват да използват нови инструменти и източници, така и на по-напредналите екипи да оценят нивото си и да идентифицират как биха могли да се подобрят.

Освен това, този доклад може да се използва заедно с наскоро пуснатото обучение на ENISA за [Оркестрация на CSIRT инструменти](#) или за провеждане на по-фокусирани партньорски проверки, използвайки [методологията за зрялост на ENISA](#).

Резултатите от проучването са разделени в три доклада и в хранилище, хоствано в GitHub. Целта е да се предложи отправна точка за нови или вече създадени екипи, които трябва да идентифицират или преоценят подходящите мерки за проактивно разкриване на инциденти.

- 1- [Доклад - Резултати от анкетата](#)
 - Проучване сред екипите за реакция при инциденти в Европа;
 - Сравнение с проучването от 2011 г.
- 2- [Доклад - Мерки и източници на информация](#)
 - Опис на наличните методи, инструменти, дейности и източници на информация;
 - Оценка на идентифицирани мерки и източници на информация.
- 3- [Доклад - препоръки за анализ на добри практики](#)
 - Анализ на събраните данни;
 - Препоръки.
- 4- [Онлайн хранилище – GitHub](#)
 - Информационни източници;
 - Мерки и инструменти.

За повече информация:

Екип за реагиране при инциденти в компютърната сигурност

<https://www.enisa.europa.eu/news/enisa-news/getting-ready-for-the-next-security-incidents>

Ето какви са новите функции за защита в Windows 10 2004

31 май 2020 г.

Актуализацията на Windows 10 от май 2020 г. предлага нови функции за защита, които включват по-добра защита от зловреден софтуер, по-лесни влизания и осигуряване на по-надеждно криптиране на безжичните връзки.

По-долу са посочени новите подобрения в сигурността, които потребителите получават в новия Windows 10 2004 и как те могат да бъдат използвани.

PUA в Microsoft Defender

Актуализацията от май 2020 г. включва нова секция „Защита на репутацията“ за Microsoft Defender, която ви позволява да блокирате потенциално нежелани приложения (Potentially Unwanted Apps - PUA), като използвате вградената антивирусна защита на Windows 10.

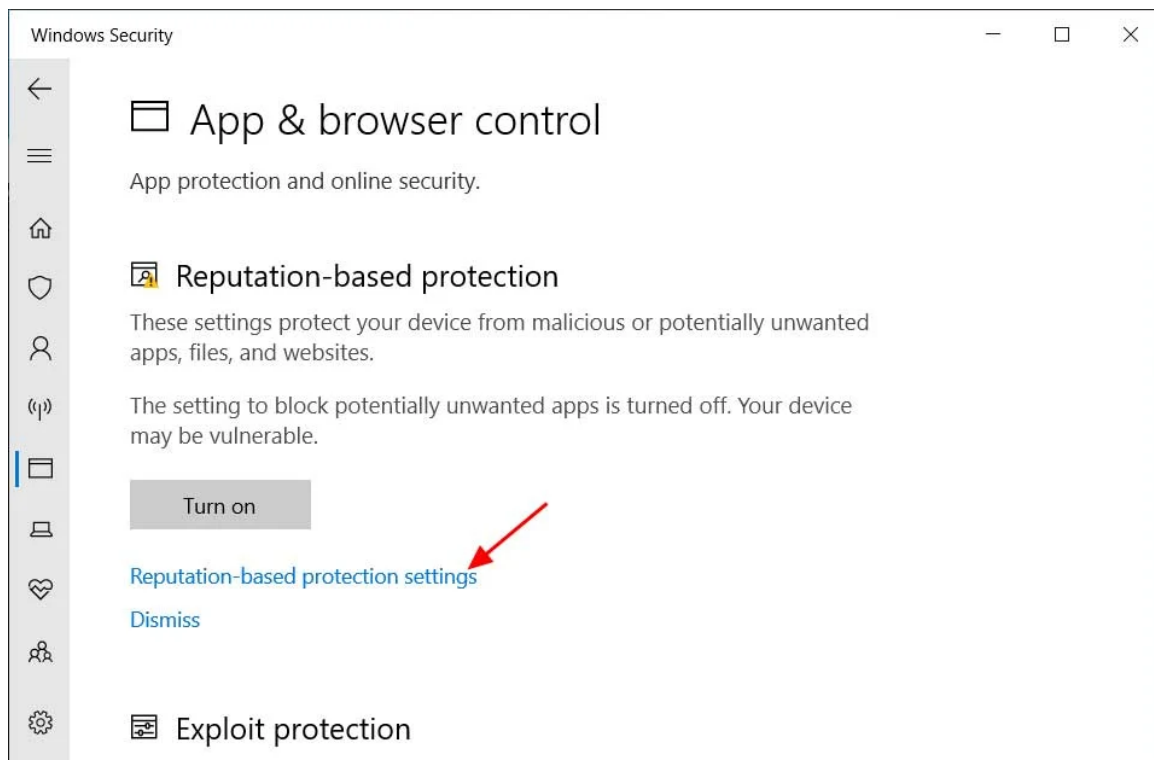
Функцията за защита от потенциално нежелани приложения е налична в Windows 10 от известно време, но тя беше скрита в настройките, които бяха достъпни само за администраторите с помощта на командата Set-MpPreference PowerShell.

С актуализацията от май 2020 г., известна още като Windows 10 2004, Microsoft заложи тази функция като част от своята защита, базирана на репутацията, в приложението Windows Security.

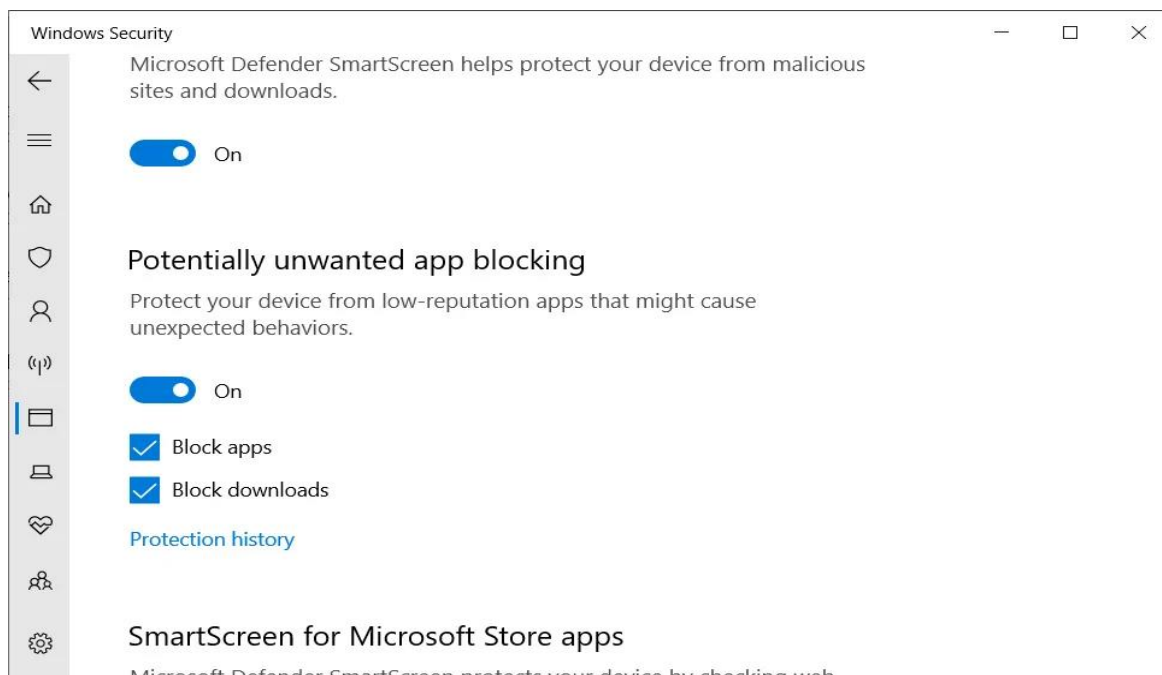
За да активирате функцията за защита от PUA в Windows 10, изпълнете следните стъпки:

1. Отворете приложението за защита на Windows (Windows Security app) от Update & Security > Windows Security.
2. Отидете на App & browser control.
3. Изберете 'Reputation-based protection settings'

Екип за реагиране при инциденти в компютърната сигурност



4. Превключете опцията "Reputation-based control" в положение „On“, за да я активирате.



Екип за реагиране при инциденти в компютърната сигурност

След като опцията бъде активирана, Windows 10 ще започне да блокира потенциално нежелани програми, които показват реклами, да променя настройките на браузъра и дори да променя системни настройки.

Под „Контрол, базиран на репутацията“, можете също така да активирате или деактивирате функциите „Блокиране на приложения“ и „Блокиране на изтегляния“ ръчно.

Опцията за блокиране на приложения активира класическата настройка „PUAProtection“, която преди това бихте могли да активирате с редактор на групови правила.

Втората опция „Блокиране на изтегляния“ използва Windows SmartScreen за блокиране на PUA, когато те се изтеглят от Chromium Microsoft Edge.

Можете да научите повече за настройките за скрита защита на Windows Defender от [тази статия](#).

Windows Hello

Актуализацията от май 2020 г. подобри функцията за удостоверяване на Windows Hello, за да предостави повече начини за нейното използване.

Потребителите на Windows 10 вече могат да използват Windows Hello, за да влязат в Safe mode, когато трябва да отстранят проблеми с компютъра.

За да активирате Windows Hello и да го използвате в Safe mode, изпълнете следните стъпки:

1. Настройте Windows Hello автентификацията от Settings > Accounts > Sign-in.
2. След като настроите Windows Hello, отидете на Settings> Update and Security> Recovery.
3. Под Advanced startup изберете Restart now.
4. В boot менюто изберете Troubleshoot > Advanced options > Startup Settings > Restart.
5. В следващото меню изберете 5 или натиснете F5, за да стартирате компютъра в Safe Mode with Networking. Можете също да изберете 4 или да натиснете 4, за да използвате Safe Mode without network.

Друго подобрение на Windows Hello ви позволява да го използвате за влизане във вашия акаунт в Microsoft.

Екип за реагиране при инциденти в компютърната сигурност

За да активирате влизане в акаунти на Microsoft без парола , изпълнете следните стъпки:







1. Отидете на Settings > Accounts > Sign-in.
2. Изберете „On“ на „Make your device passwordless“.

Windows 10 получава Wi-Fi 6 и WPA3 поддръжка

Windows 10 версия 2004 вече включва поддръжка за Wi-Fi 6 и протокола WPA3.

Новата технология Wi-Fi 6 осигурява по-висока скорост и по-добра производителност, когато имате няколко устройства, свързани към една и съща връзка.

Wi-Fi 6E brings Wi-Fi® into 6 GHz

Features	Benefits
 More, contiguous spectrum	 Gigabit speeds
 Wider channels	 Extremely low latency
 Less interference	 High capacity

За да проверите дали сте свързани с Wi-Fi 6 мрежа, следвайте тези стъпки:

1. Свържете се с Wi-Fi мрежа.
2. Изберете иконата на Wi-Fi мрежата от дясната страна на лентата на задачите и изберете Properties под името на Wi-Fi мрежата .
3. На екрана на Wi-Fi мрежата, под Properties, погледнете стойността до Protocol. Тя ще бъде Wi-Fi 6 (802.11ax), ако сте свързани с Wi-Fi 6 мрежа.

Ако използвате безжичен адаптер, който поддържа Wi-Fi 6, уверете се, че имате инсталирани най-новите драйвери за Windows 10.

Екип за реагиране при инциденти в компютърната сигурност

Microsoft е добавил и протокола за безжична защита WPA3 към Windows 10, ако се поддържа от вашия рутер.

Протоколът за защита WPA3 е проектиран да предпазва от атаки, използващи метода на грубата сила, като блокира процеса на безжична автентификация след няколко неуспешни опита за влизане в устройството. Той също така включва нови възможности за криптиране на връзки между всяко устройство и рутера.

За да видите дали сте свързани, използвайки WPA3 сигурност:

1. Свържете се с Wi-Fi мрежа.
2. Изберете иконата на Wi-Fi мрежата от дясната страна на лентата на задачите, след което изберете Properties под името на Wi-Fi мрежата.
3. На екрана на Wi-Fi мрежата, под Properties, погледнете стойността до Security type. Той ще включва WPA3, ако сте свързани с мрежа, използваща WPA3 криптиране за сигурност.

Можете да научите повече за подобренията в Wi-Fi 6 и WPA3 в [тази специална статия](#).

За повече информация:

<https://www.bleepingcomputer.com/news/microsoft/here-are-the-new-security-features-in-windows-10-2004/>

VMware поправя Fusion уязвимост, въведена с предишен пач

01 юни 2020 г.

Актуализация, пусната миналата седмица от VMware за версията на macOS на Fusion се опитва да поправи сериозна уязвимост на ескалация на привилегии, въведена от предишен пач.

VMware информира клиентите си в средата на март, че пуска пач за уязвимост с висок приоритет за ескалация на привилегии в Fusion, Remote Console (VMRC) и Horizon Client за Mac. Недостатъкът, проследен като CVE-2020-3950, може да бъде използван от нападател с привилегии на потребител, за да ескалира привилегии до root.

Екип за реагиране при инциденти в компютърната сигурност

Изследователите, които независимо докладваха проблема на VMware, Rich Mirch и Jeffball, веднага отбелязаха, че пачът е непълен. VMware потвърди няколко дни по-късно, че това е вярно.

Приблизително една седмица след пускането на първоначалния пач, VMware направи пореден опит да коригира уязвимостта, но тази втора корекция въведе нова уязвимост.

Този нов недостатък, проследяван като [CVE-2020-3957](#), се описва като time-of-check time-of-use (TOCTOU), който дава възможност на нападател с ниски права да изпълнява произволен код с root права.

VMware се опита да закърпи уязвимостта на TOCTOU във Fusion миналата седмица с пускането на версия 11.5.5, но пачове за VMRC и Horizon Client за Mac все още се очакват.

В допълнение към тази уязвимост, VMware информира клиентите си миналата седмица, че пуска актуализации за ESXi, Workstation и Fusion, за да се справи с няколко уязвимости със средна тежест, свързани с отказ от услуги (DoS).

Как да се предпазите?

Когато има налична актуализации за сигурност, не отлагайте изтеглянето ѝ.

За повече информация:

<https://www.securityweek.com/vmware-fixes-fusion-vulnerability-introduced-previous-patch>