CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 13.07.2020 г.

Съдържание

Годишен доклад на ENISA за 2019 г. за инциденти със сигурността на доверителните услуги

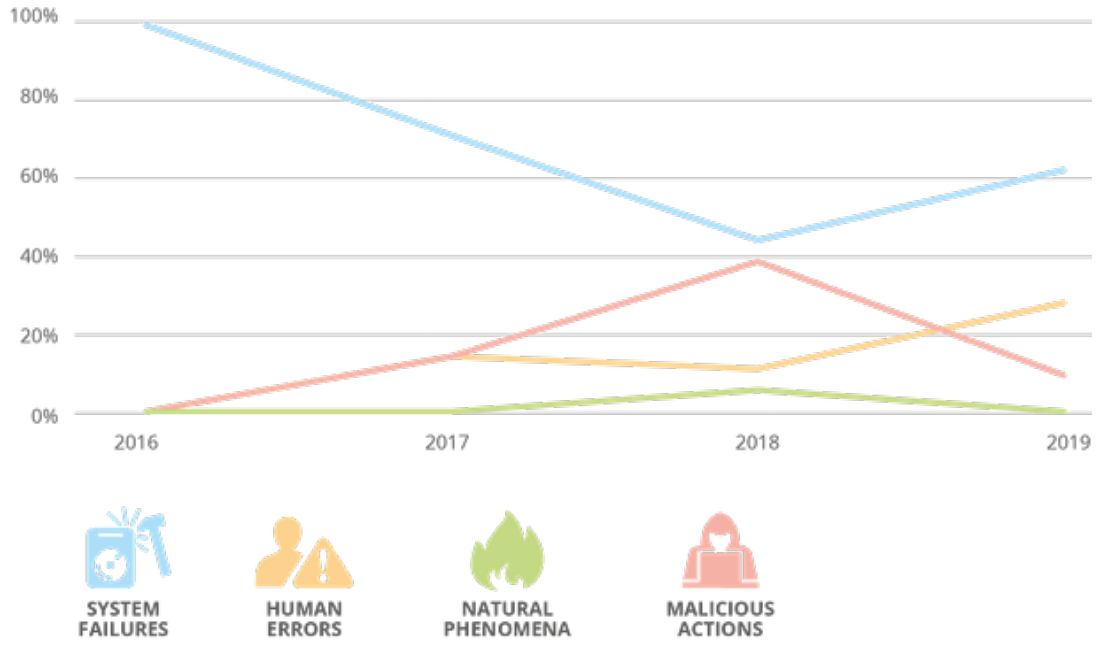
10 юли 2020 г.

За 2019 г. 27 държави от ЕС и 2 държави от ЕАСТ са съобщили за 32 инцидента със сигурността, оказали значително въздействие върху доверителните услуги в ЕС. Годишният доклад за 2019 г. дава обобщен преглед на тези нарушения в сигурността, показващи основни причини, статистика и тенденции.

Според регламента на ЕС относно електронната идентификация и доверителните услуги (eIDAS) доставчиците на доверителни услуги трябва да уведомяват своя национален надзорен орган за нарушения в сигурността. Националните надзорни органи изпращат годишни обобщени доклади за тези нарушения на ENISA и на Европейската комисия. ENISA обобщава тази информация в своите годишни доклади.

Основни изводи от доклада за инцидентите за 2019 г.:

- Значително увеличение на докладваните инциденти: увеличение с близо 80% по отношение на съобщените инциденти в сравнение с предходната година.
- Системните повреди като доминираща първопричина: те представляват повече от 60% от инцидентите и остават доминиращата първопричина през последните четири години от докладването на инциденти.
- Повечето съобщени инциденти се отнасят до квалифицирани доверителни услуги: повече от три четвърти от общите инциденти (78%) оказват влияние върху квалифицираните доверителни услуги.
- Повечето от инцидентите са незначителни: повечето инциденти са незначителни, но една трета от инцидентите (31%) са оценени като оказващи голямо въздействие. За разлика от предишните две години, през 2019 г. няма съобщения за инциденти с въздействие, оценено като катастрофално.



Основни причини за инциденти с доверителни услуги в ЕС

Общи наблюдения:

- Надзор и докладване на инциденти от неквалифицирани служби: статистиката на докладваните инциденти показва, че има недостатъчно докладване на нарушенията в сигурността на доверителните услуги.
- Докладване за уязвимости и атаки: има ясна необходимост от обмен на информация не само за действителни инциденти с въздействие на доверителната услуга на TSP, но и за атаки и уязвимости.

За достъп до доклада, моля, посетете: Годишен доклад за анализ на сигурността на доверителните услуги за 2019 г.

ENISA и наредбата за eIDAS

Агенцията за киберсигурност на ЕС ще продължи да подкрепя националните надзорни органи за прилагане на докладите за нарушения съгласно член 19 от регламента за eIDAS и да се стреми да направи този процес ефикасен, ефективен и предоставящ статистически данни. Такива данни са полезни за

надзорните органи, за органите на други сектори, както и за доставчиците на доверителни услуги и за организациите, разчитащи на тези доверителни услуги.

В тази насока ENISA наскоро пусна нов Visual Tool - CIRAS, предназначен да увеличи прозрачността относно инцидентите в киберсигурността. Онлайн визуалният инструмент, достъпен за обществеността, предоставя достъп до 4 години доклади за инциденти с доверителни услуги и до 8 години инциденти със сигурността в телекомуникационната сигурност, като се събират 1100 инцидента в киберсигурността. Новият визуален инструмент позволява и анализ на многогодишните тенденции.

Обща информация

Електронните доверителни услуги включват набор от електронни услуги около цифрови подписи, цифрови сертификати, електронни печати, времеви марки и др., използвани за осигуряване на електронни, онлайн, транзакции.

Регламентът на eIDAS е правната рамка, обхващаща целия ЕС, целяща да гарантира оперативната съвместимост и сигурността на електронните доверителни услуги в целия ЕС. Една от целите на eIDAS е да се гарантира, че електронните транзакции могат да имат същата юридическа валидност като традиционните транзакции на хартиен носител, да се създаде рамка, в която цифровият подпис да има същата стойност като ръкописен подпис.

Този регламент е важен за европейския цифров пазар, тъй като позволява на предприятията и гражданите да работят и да използват цифрови услуги в целия ЕС. Приет през юли 2014 г., регламентът за eIDAS влезе в сила през 2016 г.

Сигурността е важен стълб на цялостната рамка. Член 19 от регламента за eIDAS изисква доставчиците на доверителни услуги в ЕС да оценят рисковете, да предприемат подходящи мерки за сигурност, да смекчат нарушенията в сигурността. Те уведомяват за нарушения националните надзорни органи, които от своя страна изпращат годишни обобщени доклади за докладваните нарушения на ENISA и Комисията. ENISA публикува обобщените данни годишно.

Сигурността и доверието са ключови фактори за успеха на eIDAS. ENISA подкрепя Европейската комисия и държавите-членки на ЕС в прилагането на изискванията за сигурност на регламента за eIDAS и подкрепя сътрудничеството и обмена на информация между националните надзорни органи в Европа относно сигурността на доверителните услуги.

За повече информация:

https://www.enisa.europa.eu/news/enisa-news/annual-report-on-trust-services-security-incidents-in-2019

Критичен пропуск, разкрит в софтуера Zoom за Windows 7 или по-ранни версии

10 юли 2020

В софтуера за видеоконференции на Windows е установена 0-day уязвимост, която може да позволи на нападателя да изпълни произволен код на компютъра на жертвата, използваща Microsoft Windows 7 или по-стара версия.

За да се възползва успешно от уязвимостта, всичко, което атакуващият трябва да направи, е да подмами потребител на Zoom да извърши някакво типично действие като отваряне на получен файл. По време на атаката на потребителя не се задейства или показва предупреждение за сигурност.

Тази уязвимост е експлоатируема само в Windows 7 и по-ранни версии на Windows. Вероятно е използваема и на Windows Server 2008 R2 и по-ранни, въпреки че тестове все още не са извършени.

Въпреки че Microsoft преустанови официалната поддръжка на Windows 7 този януари и насърчи потребителите да преминат към по-защитени версии на операционната система, Windows 7 все още се използва широко от потребителите и организациите.

Изследователите от Acros Security, създателите на 0patch, са разработили микро пачове за всички версии на Zoom Client за Windows (започвайки с версия 5.0.3 и всички до най-новата версия 5.1.2), за да разрешат проблема със сигурността и ги пуснаха безплатно.

Когато потребителят активира 0patch в своята система, злонамереният код, изпратен от нападател, не се изпълнява, когато Zoom потребител натисне бутона "Start Video".

Zoom Client разполага с достатъчно устойчива функция за автоматично актуализиране, която поддържа домашните потребители актуализирани, освен ако те наистина не желаят да бъдат такива.

Въпреки това, администраторите на фирми често обичат да поемат контрола над актуализациите и може да ползват по-стари версии, в които не са отстранени грешки в сигурността.

Какво трябва да направят засегнатите потребители?

Потребителите могат да внедрят микропача, пуснат от Acros Security, но тъй като той идва от софтуерна компания на трета страна, а не от самия Zoom, не е препоръчително да го правят.

Zoom потвърди, че уязвимостта, спомената по-горе, вече е закърпена с версия на Zoom 5.1.3.

Потребителите могат да се защитят, като приложат актуализации или изтеглят най-новия софтуер Zoom с всички актуализации за сигурност от https://zoom.us/download.

Само през изминалия месец Zoom адресира две критични уязвимости в своя софтуер за видеоконференции на Windows, macOS или Linux компютри, които биха могли да позволят на нападатели да хакнат системите на участници в групов чат или на отделен получател.

През април в Zoom бяха разкрити и докладвани поредица от проблеми, които повдигнаха опасенията за поверителност и сигурност около софтуера за видеоконференции сред милиони потребители.

По-рано тази година Zoom направи сериозна грешка в поверителността на софтуера си, която можеше да позволи на неканени участници да се присъединят към частни срещи и да подслушват дистанционно частни аудио и видео разговори или документи, споделяни по време на сесията.

За повече информация:

https://thehackernews.com/2020/07/zoom-windows-security.html

Доклад: Най-популярните домашни рутери съдържат „критични“ недостатъци

10 юли 2020 г.

Често срещаните устройства на Netgear, Linksys, D-Link и други съдържат сериозни уязвимости в сигурността, които не са коригирани дори в актуализации.

Преглед на сигурността на 127 популярни домашни рутери установи, че повечето съдържат поне един критичен недостатък.

„Докладът за сигурност на рутерите“ (PDF) от Peter Weidenbach и Johannes vom Dorp - и двамата от Fraunhofer Institute - установи, че не само всички рутери, които те разглеждат, имат недостатъци, а много от тях са засегнати от стотици известни уязвимости.

Рутерите, анализирани - от доставчици като D-Link, Netgear, ASUS, Linksys, TP-Link и Zyxel – средно са засегнати от 53 критични уязвимости (CVE), като дори най-„безопасното“ устройство е с 21 CVE, според доклада. Изследователите не изброяват в доклада специфичните уязвими места.

Рутерите биват разгледани в няколко основни аспекта: актуализации на устройствата, версия на операционната система и всички известни критични уязвимости, засягащи ги; използвани техники за смекчаване от доставчиците и колко често ги активират; наличие на частен криптографски ключов материал във фърмуера на рутера; и наличие на кодирани идентификационни данни за вход.

В обобщение, анализът показва, че няма рутер без недостатъци и няма производител, който да върши перфектна работа във всички аспекти на сигурността.

Въпреки че хората правят често срещани грешки при конфигурирането на домашните рутери - което води до проблеми със сигурността - те не са основната причина за липсата на сигурност, открита сред устройствата.

Изследователите използват автоматизиран подход за проверка на най-новите версии на фърмуера в пет аспекта, свързани със сигурността.

91 процента от рутерите работят под Linux. Въпреки че Linux може да бъде много сигурна ОС на теория, изследователите откриват, че много от рутерите са захранвани от много стари версии на Linux, които не разполагат с поддръжка и по този начин имат много проблеми.

Повечето устройства все още се захранват с 2.6 Linux ядро, което вече не се поддържа в продължение на много години. Това води до голям брой критични и с висока тежест CVE, засягащи тези устройства.

Друг ключов проблем, засягащ сигурността на рутерите, е, че фърмуерът на устройството не се актуализира толкова често, колкото трябва. Въпреки това дори актуализациите на фърмуера на рутера не решават проблемите в много от случаите.

Изглежда, че някои доставчици дават приоритет на сигурността малко повече от други. AVM International е най-добрата група по отношение на всички изследвани аспекти на сигурността, въпреки че рутерите на компанията също съдържат недостатъци.

ASUS и Netgear също дават приоритет на няколко аспекта в сигурността на устройствата повече от някои от другите доставчици. И двамата производители актуализират своите рутери по-често от своите конкурентни компании и използват по-актуални, поддържани версии на ядрото на Linux за своя фърмуер.

За повече информация:

https://threatpost.com/report-most-popular-home-routers-have-critical-flaws/157346/