CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 13.04.2020 г.

Съдържание

Критичен бъг във VMware разкрива на хакери важна корпоративна информация

10 април 2020

Бъгът, оценен с тежест 10, потенциално засяга голям брой корпоративни виртуални машини и хостове.

Критичният бъг в услугата Directory VMware (vmdir) може да разкрие съдържанието на цялата корпоративна виртуална инфраструктура, ако бъде експлоатиран.

Vmdir е част от vCenter сървъра на VMware, който осигурява централизирано управление на виртуализирани хостове и виртуални машини (VMs) от една конзола. Според описанието на продукта, един администратор може да управлява стотици натоварвания.

Тези натоварвания се управляват от механизма за влизане „single sign-on“ (SSO), за да се улесни работата на администраторите; вместо да се налага да влизат във всеки хост или VM с отделни идентификационни данни, за да получат видимост за него, един механизъм за удостоверяване работи в цялата конзола за управление.

Vmdir от своя страна е централен компонент на vCenter SSO (заедно със Security Token Service, администраторски сървър и vCenter Lookup Service). Също така, vmdir се използва за управление на сертификати за работните натоварвания, управлявани от vCenter.

Критичният недостатък (CVE-2020-3952) е разкрит и пачнат на 9 април; той е оценен с 10 от 10 по скалата за тежест на уязвимостта на CVSS v.3. Въпросният бъг е лошо реализиран контрол на достъпа, който може да позволи на злонамерен участник да заобиколи механизмите за удостоверяване.

При определени условия vmdir, който се доставя с VMware vCenter Server, като част от вграден или външен контролер на платформа услуги (PSC), не прилага правилно контролите за достъп.

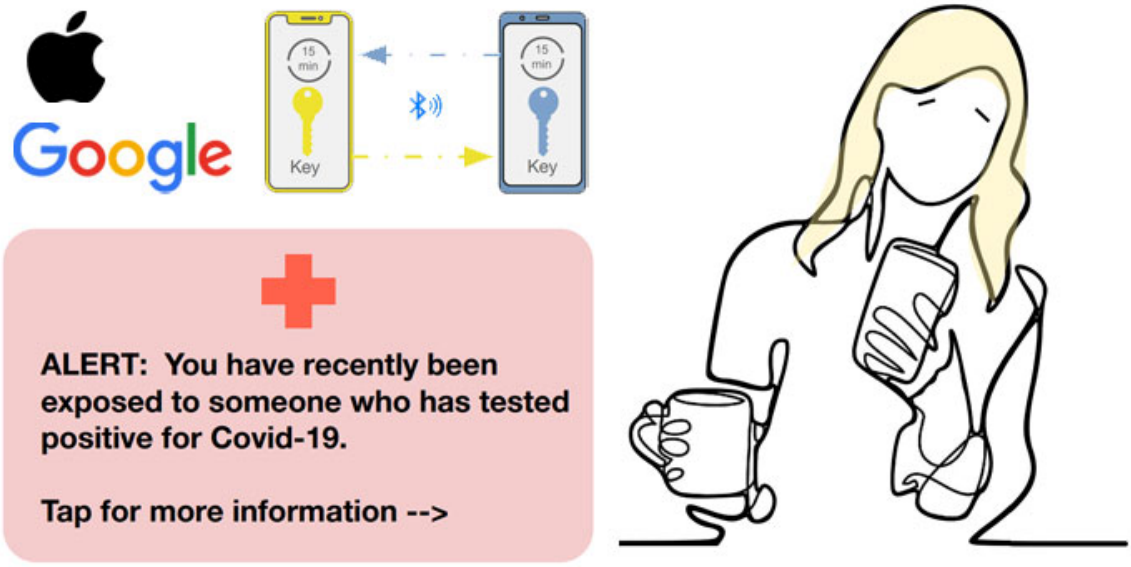
Що се отнася до вектора на атаката, злонамерен участник с достъп до мрежата до засегнатото vmdir разгръщане може да извлече високо чувствителна информация. От своя страна тази информация може да се използва за компрометиране на самия vCenter Server или други услуги, които зависят от vmdir за удостоверяване.

Насърчават се администраторите да приложат пачовете възможно най-скоро.

За повече информация:

https://threatpost.com/critical-vmware-bug-corporate-treasure-hackers/154682/

Google и Apple планират да превърнат телефоните в COVID-19 проследяващи устройства



10 април 2020

Тех- гигантите Apple и Google обединиха усилията си, за да разработят оперативно съвместим инструмент за проследяване, който ще помогне на хората да определят дали са влезли в контакт с някой, заразен с COVID-19.

Като част от тази нова инициатива се очаква компаниите да пуснат API, което публичните агенции да могат да интегрират в своите приложения. Следващата итерация ще бъде вградена платформа на системно ниво, която използва Bluetooth low energy (BLE) , за да се даде възможност за проследяване.

Очаква се приложенията да бъдат налични в средата на май за Android и iOS, като по-широката система за проследяване ще бъде въведена през следващите месеци.

"Поверителността, прозрачността и съгласието са от изключително значение в тези усилия. Очакваме с нетърпение да изградим тази функционалност след консултация със заинтересованите страни", заявиха от компаниите.

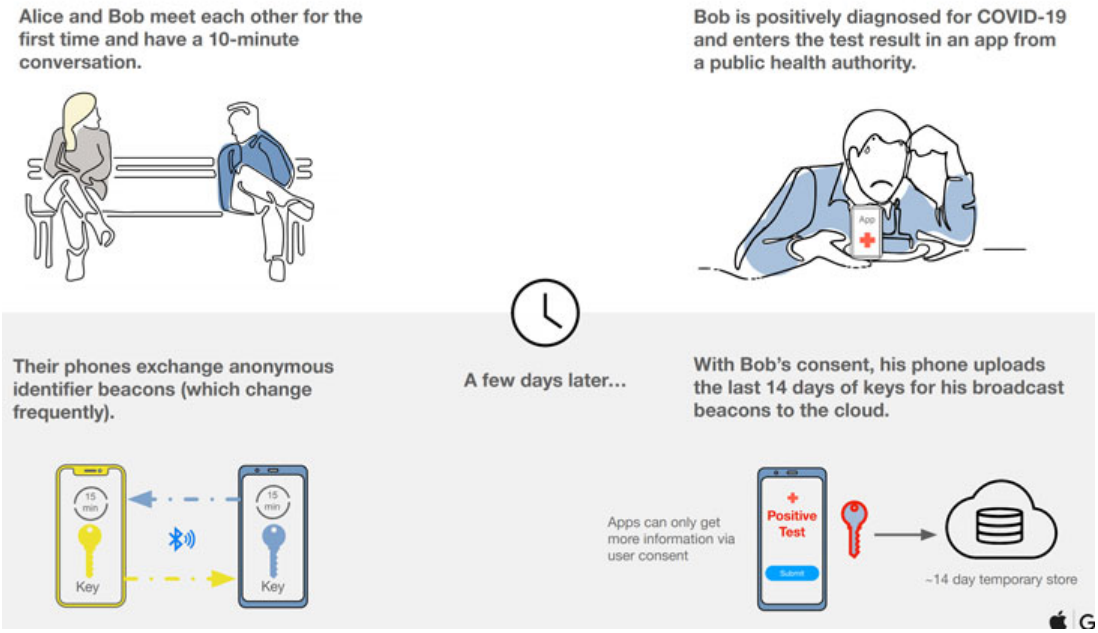
Рядкото сътрудничество е наложително, тъй като правителствата по целия свят все повече се обръщат към технологии като проследяване на телефона и разпознаване на лица, за да се борят с вируса и с неговите огнища.

Apple също пусна нова уеб страница, обявяваща тази функция, в която подробно са описани предварителните спецификации на Bluetooth, спецификациите за криптография и рамковото API, на което ще се основава системата за проследяване.

Нулева употреба на данните за местоположението

За разлика от съществуващите приложения, разработени от различни държави, които използват проследяване на местоположението в реално време, за да прилагат карантинните правила, предложената система не включва проследяване на местоположенията на потребители или други идентификационни данни.

Вместо това приложеинието използва друг механизъм, за да идентифицира дали човек е бил около други хора, които са тествали положителен COVID-19, като по този начин гарантира, че личната неприкосновеност на личния живот не е нарушена.



Както Apple, така и Google подчертаха, че потребителите ще трябва да дадат своето изрично съгласие за работата на приложението. Това означава, че за да бъде то

ефективно, милиони хора ще трябва да се включат, което налага Apple и Google да създадат адекватни защитни мерки за поверителност, преди приложението да бъде масово внедрено.

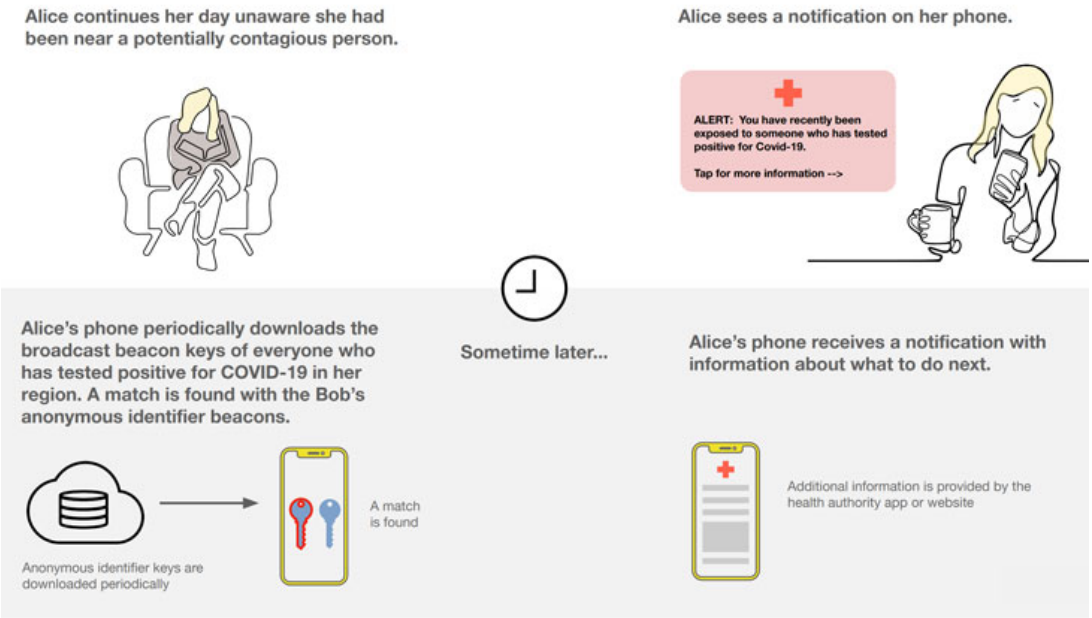
Според бяла книга, публикувана от Google, ето как може да работи такава система:

- Когато двама души са в близък контакт за определен период от време (да речем 10 минути или повече), техните телефони ще обменят анонимни идентификатори. Идентификаторите се обменят на всеки 15 минути и не съдържат лична информация.
- Ако едно от двете лица е положително диагностицирано за COVID-19, то може да въведе резултата от теста в приложение на орган за обществено здраве, който е интегрирал гореспоменатото API.
- Тогава заразеният може да даде съгласие да качи последните 14 дни от своите излъчвани маяци в системата.
- След това всеки друг човек, който е бил в непосредствена близост до индивидуално тествания положителен, ще бъде предупреден, и ще бъдат сигнализирани всички, които са били в региона, в който има положително тествани за COVID-19.
- След това приложението ще предоставя индивидуална информация за следващите стъпки.

Системата на Apple и Google е по линия на TraceTogether - приложение, разработено от правителствени служители на Сингапур, за да се даде възможност за проследяване на контакти чрез Bluetooth.

Приложението, което вече е с отворен достъп, използва Bluetooth Relative Signal Strength Indicator (RSSI) между устройствата, за да определи близостта и продължителността на среща между двама души. Записите на срещите се съхраняват в съответните им телефони 21 дни.

Приложения като COVID-Watch и Private Kit на MIT: Безопасни пътища, също разчитат на комбинация от GPS и Bluetooth данни, за да проследяват хора в продължение на 14 дни.



Притеснения за поверителността при пандемично наблюдение

Необходимостта от отделяне на заразени лица и поддържане на карантина накара правителствата по целия свят да предприемат строги мерки за наблюдение.

В отговор на опасенията за поверителност, повдигнати от Европейския надзорен орган по защита на данните, Европейският съюз заяви, че ще възприеме "общоевропейски подход" за използване на мобилни приложения за проследяване на разпространението на коронавируса и ще включи обща схема за използване на анонимни, обобщени данни за проследяване на хората, които влизат в контакт със заразените и за наблюдение на хората под карантина.

По-рано тази седмица Американският съюз за граждански свободи (ACLU) изрази опасения относно проследяването на потребителите с обобщени телефонни данни, като се аргументира, че всяка система ще трябва да бъде ограничена по обхват и да избягва всякакво нахлуване и злоупотреби с личния живот.

Трябва да бъде определено колко дълго ще продължи събирането на данни и кога ще бъдат изтрити. Важно е също така да се гарантира, че събраните анонимни данни не могат да бъдат използвани отново, за да се проследяват хора.

Експертът по киберсигурност Брус Шнайер заяви, че всяка инициатива за събиране на данни и дигитален мониторинг "трябва да бъде научно обоснована и считана за необходима от експертите по обществено здраве с цел ограничаване. И че обработката на данни трябва да е пропорционална на нуждата".

В надпреварата за ограничаване на разпространението и контрола на ситуацията, мобилизирането на пандемичен апарат за наблюдение, който да помогне за овладяване на огнището, изисква адекватен баланс между прозрачност, удовлетворяване на нуждите на общественото здраве и гражданските права.

За повече информация:

https://thehackernews.com/2020/04/iphone-android-coronavirus-tracing.html

„Критичен съвет за сигурност“ на Cisco част от фишинг кампания

Фишинг атака, прикрита зад „Критична актуализация“ на Cisco откradва удостоверения на Webex

11 април 2020 г.

С нарастването на онлайн срещите и продължаващите фишинг кампании, все повече и повече потребители са засегнати от подправен съвет за сигурност на Cisco, който предупреждава за критична уязвимост и допълнително призовава жертвите да

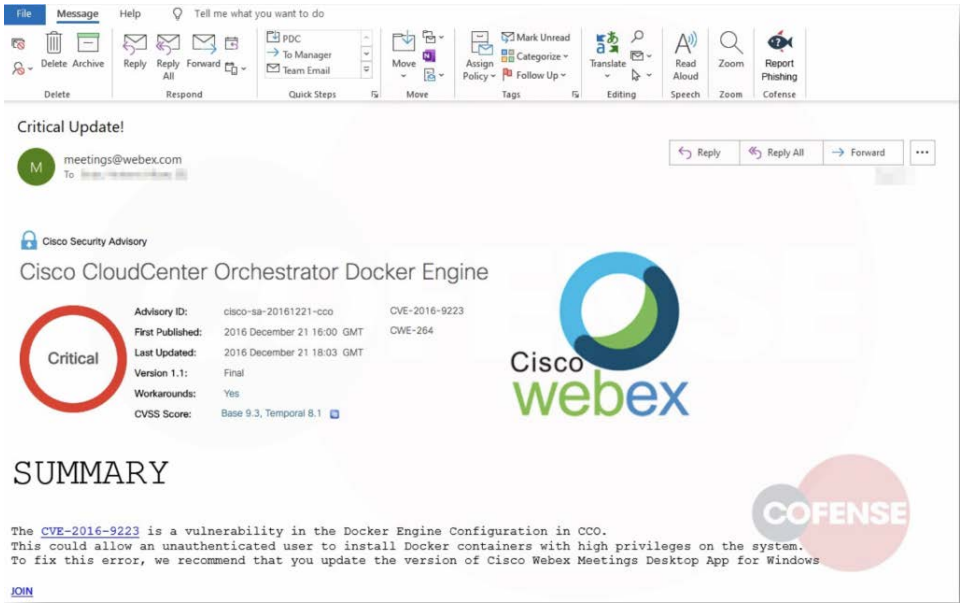
"актуализират", като единствената му цел е да бъдат откраднати пълномощията за Webex платформата за конференции на Cisco.

Изследователите са на мнение, че фишинг имейлите се изпращат с различни теми, привличащи вниманието, например "Критична актуализация" или "Предупреждение!" и произхождат от измамния имейл адрес, " meetings@ webex [.] com".

Това е мащабна фишинг кампания, като многобройни крайни потребители от няколко няколко индустрии, включително здравната и финансовата, докладват за имейла. Тялото на имейла има съдържание на истински съветник за сигурност на Cisco от декември 2016 г., съдържа и марката на Cisco Webex.

Съветникът за сигурност е за CVE-2016-9223, законна уязвимост в CloudCenter Orchestrator Docker Engine, която е инструмент за управление на Cisco за приложения в много центрове за обработка на данни, частни облаци и отворени облачни инфраструктури.

Имейлът съдържа следното съобщение към жертвите: „За да коригирате тази грешка, препоръчваме ви да актуализирате версията на приложението Cisco Meetings Desktop за Windows“ и ги насочва към бутон „Присъединяване“, за да се запознаят с „актуализацията“.



Нападателите, стоящи зад тази кампания, се фокусират върху детайлите, чак до URL адреса, свързан с бутона „Присъединяване“. Предпазливите получатели на електронна поща, които задържат курсора върху бутона, за да проверят URL адреса,

ще открият, че URL адресът [[hxxps://globalpagee-goad webex[.]com/signin] е поразително подобен на автентичния URL адрес на Cisco WebEx [hxxps://globalpage-prod[.]webex[.]com/signin].

След това жертвите, които кликнат върху бутона „Присъединяване“, биват пренасочени към фишинг целевата страница, която е идентична с реалната страница за вход в Cisco WebEx.

Изследователите съобщават, че има една малка разлика в това, че когато имейл адресите се въвеждат в автентичната страница на Webex, записите се проверяват, за да се потвърди дали има свързани акаунти. На фишинг страницата междувременно всеки запис на формат на имейл отвежда бенефициента направо на следващата страница, за да поиска парола.

Следователно изследователите предупреждават потребителите да останат нащрек.

За повече информация:

https://www.ehackingnews.com/2020/04/cisco-critical-security-advisory-part.html