CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 24.09.2020 г.

Съдържание

Незащитен сървър на Microsoft Bing разкрива заявките за търсене и местоположението на потребители

22 септември 2020 г.

Вътрешен сървър, свързан с Microsoft Bing, разкрива чувствителни данни на потребителите на мобилни приложения на търсачката, включително заявки за търсене, подробности за устройството, GPS координати и други.

Базата данни обаче не включва никакви лични данни като имена или адреси.

Изтичането на данни, открито на 12 септември, представлява огромен 6,5TB кеш от регистрационни файлове, който е достъпен за всеки без никаква парола, което потенциално позволява на киберпрестъпниците да използват информацията за извършване на изнудване и фишинг измами.

Според WizCase, за сървъра Elastic се смята, че е бил защитен с парола до 10 септември, след което удостоверяването изглежда неволно е премахнато.

Неправилно конфигурираните сървъри са постоянен източник на изтичане на данни през последните години, което води до разкриване на имейл адреси, пароли, телефонни номера и лични съобщения.

Въз основа на огромното количество анализирани данни може да се предположи, че всеки, който е направил търсене в Bing с мобилното приложение, докато сървърът е бил незащитен, е изложен на риск.

Освен данните за устройството и местоположението, данните се състоят и от точното време на извършване на търсенето с помощта на мобилното приложение, частичен списък на URL адресите, които потребителите са посетили от резултатите от търсенето, и три уникални идентификатора като ADID, „deviceID“ и „devicehash“.

В допълнение, сървърът също е попаднал под така наречената "meow attack" поне два пъти, автоматизирана кибератака, която е изтрила данни от над 14 000 незащитени копия на бази данни от юли без обяснение.

Въпреки че незащитеният сървър не разкрива имена и друга лична информация, WizCase предупреди, че данните могат да бъдат използвани за други неблагоприятни цели, в допълнение към излагането на потребителите на физически атаки, позволявайки на престъпниците да определят местонахождението им.

След като хакерът получи заявката за търсене, би могло да бъде възможно да се установи самоличността на потребителя и благодарение на всички налични подробности на сървъра да го направи лесна цел за изнудване.

За повече информация:

https://thehackernews.com/2020/09/bing-search-hacking.html

Девети семинар ENISA-EC3 за сътрудничество CSIRTs-LE: рамо до рамо за противодействие на киберпрестъпността

22 септември 2020 г.

На 16 септември 2020 г. Агенцията на Европейския съюз за киберсигурност ENISA и Европейският център за киберпрестъпления EC3 организираха 9-ия годишен семинар за CSIRTs - по-специално национални и правителствени (n / g) CSIRTs (Екипи за реагиране при инциденти в компютърната сигурност) и техните колеги LE (правоприлагащи органи).

CSIRTs и LE общностите от страните от ЕС и ЕАСТ, заедно с представители на институциите и органите на ЕС и Съвета на Европа, се срещнаха, за да обсъдят начини за ефективно сътрудничество с цел противодействие на киберпрестъпността. Благоприятните условия за киберпрестъпления, причинени от пандемията от COVID-19, само направиха тази среща още по-важна. В тазгодишният семинар взеха участие само организации, получили специална покана. В резултат на ситуацията с COVID-19, общностите CSIRT и LE трябваше да координират своите реакции и да реагират на атаките, насочени, например, към здравния сектор, който вече е изправен пред критична ситуация поради пандемията.

По време на семинара участниците имаха възможност и да споделят истории за успех и да представят национални примери за сътрудничество и управление на кризи, както и инициативи от институции и органи на ЕС. Експертите обсъдиха съответните политически разработки на ЕС, рамки за сътрудничество и механизми за реагиране срещу кибер заплахите.

Основните изводи на семинара бяха, че доверието е крайъгълният камък на сътрудничеството между CSIRTs и LE и че съдебната власт трябва да бъде включена на ранен етап от реакцията при атака. Събитието също така подчерта, че е от съществено

значение да има законова и политическа рамка и необходимите инструменти и процедури. И накрая беше констатирано, че кризите предлагат уникална възможност за тестване на сътрудничеството между CSIRTs и LE и за идентифициране на пропуски.

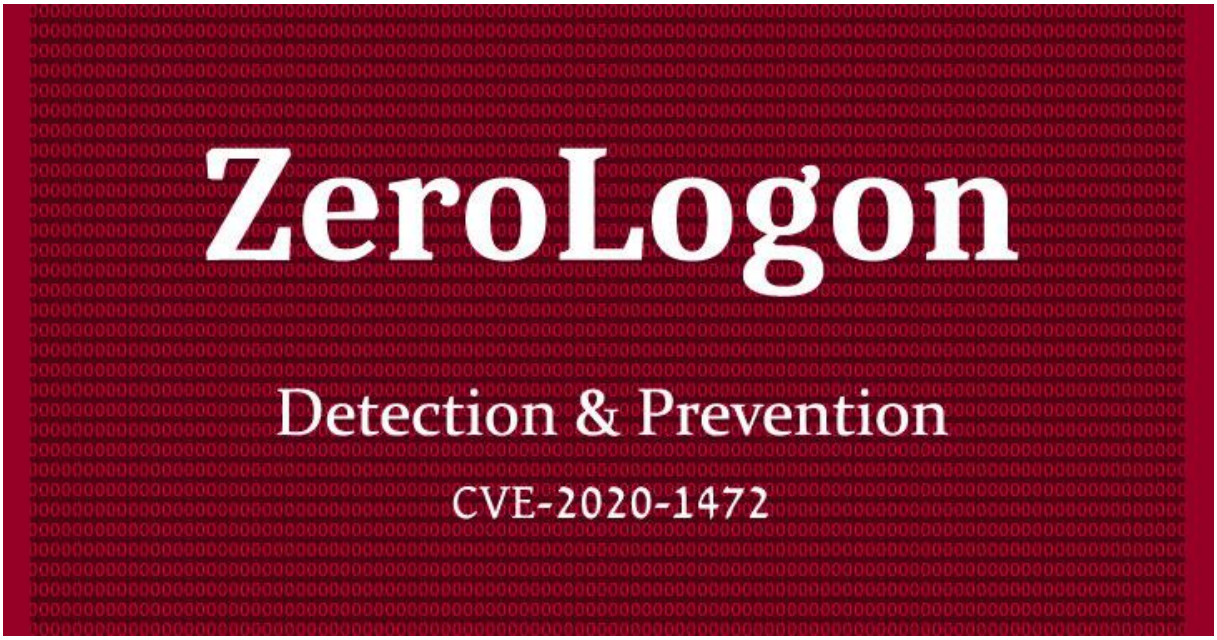
Докладът на ENISA за 2020 г. относно сътрудничество между CSIRTs и LE, който се очаква да бъде финализиран до края на 2020 г., ще бъде публикуван в раздела за публикации на уебсайта на ENISA.

Линк към новината:

https://www.enisa.europa.eu/news/enisa-news/ninth-enisa-ec3-workshop-on-csirt-le-cooperation-standing-shoulder-to-shoulder-to-counter-cybercrime

Откриване и предотвратяване на критичната уязвимост ZeroLogon на Windows Server

23 септември 2020 г.



Ако администрирате Windows Server, уверете се, че е актуализиран с всички скорошни корекции, издадени от Microsoft, особено тази, която коригира наскоро поправена критична уязвимост, която може да позволи на неупълномощени хакери да компрометират контролера на домейна.

Наречена „Zerologon“ (CVE-2020-1472), уязвимостта за ескалация на привилегиите съществува поради несигурното използване на AES-CFB8 криптиране за сесии Netlogon, което позволява на отдалечените хакери да установят връзка с целевия контролер на домейн през отдалечения протокол Netlogon (MS-NRPC).

Атаката използва недостатъци в протокола за удостоверяване, който потвърждава автентичността и идентичността на компютър, свързан с домейн, към Контролера на домейни. Поради неправилното използване на AES режим на работа е възможно да се подправи самоличността на всеки компютърен акаунт (включително тази на самия DC) и да бъде зададена празна парола за този акаунт в домейна.

Въпреки че уязвимостта с CVSS тежест 10,0, беше разкрита за първи път на обществеността, когато Microsoft пусна пач за нея през август, тя стана обект на внезапна загриженост, след като изследователите публикуваха технически подробности и доказателство за концепцията на недостатъка миналата седмица .

Заедно с индийските и австралийските правителствени агенции, Американската агенция за киберсигурност и сигурност на инфраструктурата (CISA) издаде спешна директива, с която нареди на федералните агенции незабавно да поправят недостатъците на Zerologon на Windows сървърите.

Чрез изпращане на редица съобщения в Netlogon, в които различни полета се запълват с нули, неупълномощен нападател може да промени компютърната парола на контролера на домейна, който се съхранява в AD. След това може да се използва за получаване на идентификационни данни на администратора на домейна и след това възстановяване на оригинална парола за DC.

Според Secura, споменатият недостатък може да бъде използван в следната последователност:

- Подправяне на идентификационните данни на клиента
- Деактивиране на подписването и запечатването на RPC
- Подправяне на разговор
- Промяна на AD парола на компютъра
- Промяна на администраторска парола за домейн

Уязвимостта изисква незабавни и спешни действия.

Ако засегнатите контролери на домейни не могат да бъдат актуализирани, уверете се, че са премахнати от мрежата.

Нещо повече, Samba - приложение на SMB мрежов протокол за Linux системи - версии 4.7 и по-стари също са уязвими към недостатъка Zerologon. Издадена е и актуализация за корекция за този софтуер.

Освен обяснението на основната причина за проблема, Cynet публикува и подробности за някои критични артефакти, които могат да се използват за откриване на активна експлоатация на уязвимостта, включително специфичен модел на памет в паметта lsass.exe и необичаен скок в трафика между lsass.exe.

За да позволят на потребителите на Windows Server бързо да откриват свързани атаки, експертите пуснаха правилото YARA, което може да открива атаки, възникнали преди неговото внедряване, докато за мониторинг в реално време е наличен и прост инструмент за изтегляне.

За да отстранят изцяло проблема обаче, на потребителите се препоръчва да инсталират най-новата актуализация на софтуера от Microsoft възможно най-скоро.

За повече информация:

https://thehackernews.com/2020/09/detecting-and-preventing-critical.html