CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

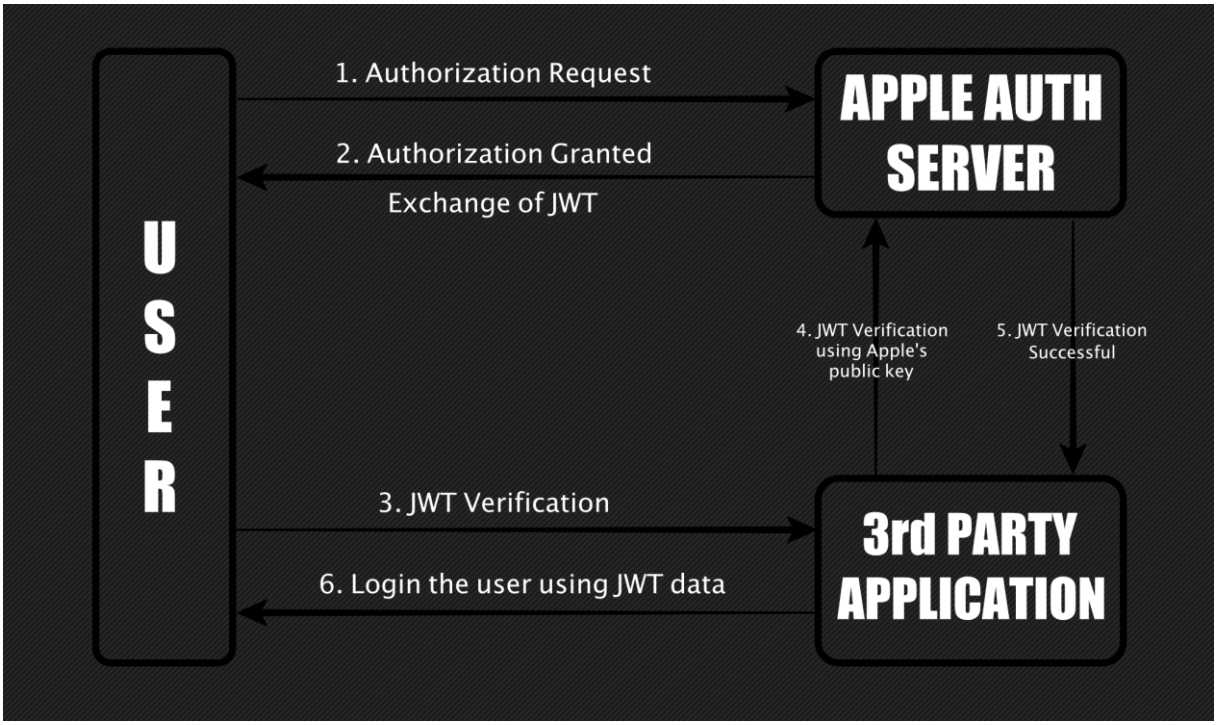
Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 02.06.2020 г.

Съдържание

Apple плаща бонус в размер на 100 000 щатски долара за открит критичен недостатък в „Sign in with Apple“

1 юни 2020 г.



Apple отстрани критичен недостатък във функцията си „Sign in with Apple“, с който би могло да бъде злоупотребено. Наскоро изследовател откри критичната уязвимост и е получил 100 000 долара за нея.

Недостатъкът произтича от функцията „Sign in with Apple“, която беше въведена от Apple на световната конференция за разработчици миналата година. Функцията има за цел да улесни и да направи по-сигурен входът на потребителите на Apple в приложения и уебсайтове на трети страни.

Един от акцентите на „Sign in with Apple“ е, че потребителите могат да се регистрират за услуги на трети страни, без да се налага да разкриват своя Apple ID имейл адрес за тези услуги. Това работи, тъй като влизането в Apple първо валидира потребителите от страна на клиента, а след това инициира заявка за JSON Web Token (JWT) от услугите за удостоверяване на Apple. Този JWT се използва от приложението на третата страна за потвърждаване на самоличността на потребителя.

Проблемът е, че след като Apple потвърди потребителя чрез Apple ID имейл адреса, той не потвърждава дали заявката за JWT е от този действителен потребителски акаунт. Атакуващият може да злоупотреби с този недостатък, като предостави Apple ID имейл, който принадлежи на жертвата и да заблуди сървърите на Apple, за да генерира валиден JWT payload. След като нападателят направи това, той може да влезе в приложение на трета страна.

Недостатъкът може да бъде експлоатиран, дори ако потребителите са решили да скрият своите имейл идентификатори от трети страни. Може да се използва и за регистриране на нови акаунти с идентификационни номера на Apple жертвите.

Има две защити, които нападателите трябва да прескочат, за да осъществят нападение. Първо, те се нуждаят от имейл идентификатор за потребител на Apple - макар че това може да бъде имейл идентификатор на всеки потребител на Apple. Второ, те трябва да влязат в приложение на трети страни чрез Sign in with Apple, което не изисква допълнителни мерки за сигурност.

Въздействието на тази уязвимост е критично, тъй като може да позволи пълно поглъщане на акаунта. Много разработчици са интегрирали Sign in with Apple в своите услуги, включително Dropbox, Spotify, Airbnb и Giphy. Тези приложения не са тествани, но биха могли да бъдат уязвими при цялостно поглъщане на акаунт, ако няма други мерки за сигурност при проверката на потребител.

Apple е провела разследване на регистрационните файлове и е определила, че няма злоупотреба или компромис с профил поради тази уязвимост. Изследовател открива този недостатък през април и го съобщава чрез програмата на Apple за бъгове, което му носи 100 000 долара.

Как да се предпазите?

Актуализирайте софтуера си, за да сте сигурни, че пачовете, налични в последната версия, ще бъдат приложени.

За повече информация:

https://threatpost.com/apple-100k-bounty-critical-sign-in-with-apple-flaw/156167/

Github разкри злонамерен „Octopus " скенер, насочен към разработчиците на софтуер

01 юни 2020 г.

GitHub разкри форма на злонамерен софтуер, който се разпространява чрез заразени хранилища в системата.

Зловредният софтуер се нарича Octopus скенер и е насочен към Apache NetBeans, която е интегрирана среда за разработка, използвана за писане на Java софтуер. Зловредният софтуер дебне в хранилищата на изходния код, качени на неговия сайт, активира се, когато програмист изтегли заразено хранилище и го използва за създаване на софтуерна програма.

След съвет от изследовател по сигурността от 9 март, сайтът, собственост на Microsoft, анализира софтуера, за да разбере как работи.

GitHub е онлайн услуга, базирана на Git, система за версия на кодове, разработена от създателя на Linux Линус Торвалдс. Git позволява на разработчиците да правят снапшоти на файлове в своите проекти за разработка на софтуер, което им позволява да възстановят промените си по-късно или да създадат различни клонове на проект, по които да работят различни хора. GitHub им позволява да добавят копия на тези хранилища към своята онлайн услуга, така че другите разработчици да могат да ги изтеглят (клонират) и да работят и върху тях.

Как работи

Разработчикът изтегля проект от хранилище, заразено от софтуера и го изгражда, което означава, че използва изходния код за създаване на работеща програма. Процесът на изграждане активира зловредния софтуер. Той сканира компютъра на жертвата, за да провери дали имат инсталиран IDB на NetBeans. Ако няма инсталиран, софтуерът няма да предприеме допълнителни действия. Но ако има, той заразява вградените файлове с dropper, който доставя крайния си payload: троянец за отдалечен достъп (RAT), който дава на извършителите контрол върху машината на потребителя. Зловредният софтуер се опитва да блокира и всеки нов проект, който се опитва да замени заразения, като по този начин се запазва в заразената система.

Octopus скенерът обаче не само заразява вградените файлове. Повечето от вариантите, които GitHub намира в своите сканирания, заразяват и изходния код на проекта, което означава, че всички други новозаразени проекти в отдалечени хранилища, ще разпространяват зловредния софтуер допълнително в GitHub.

GitHub Security Labs сканира хранилищата на сайта и откри 26 от тях, съдържащи зловреден софтуер. Екипът съпостави зловредния софтуер, който намери, със софтуерните хешове на VirusTotal и откри ниска степен на откриване, което му позволява да се разпространява, без лесно да бъде хванат.

GitHub редовно залавя хора, използващи неговите хранилища, за да разпространяват умишлено зловреден софтуер. Обикновено GitHub може просто да затвори тези хранилища и да изтрие акаунтите, но Octopus Scanner е по-сложен, защото разработчиците, притежаващи хранилищата (известни като поддръжници), не са знаели, че са заразени. Те са изпълнявали законни проекти, така че блокирането на тези акаунти или хранилища може да повлияе на бизнеса. GitHub не можеше просто да изтрие заразените файлове в компрометирано хранилище, тъй като файловете биха били от решаващо значение за законния софтуерен проект.

GitHub заяви, че е изненадан да види злонамерения софтуер, насочен към NetBeans.

Тъй като първично заразените потребители са разработчици, достъпът, който се получава, представлява голям интерес за атакуващите, тъй като разработчиците обикновено имат достъп до допълнителни проекти, производствена среда, пароли за бази данни и други критични активи. Има огромен потенциал за ескалиране на достъпа, което е основна цел на атакуващия в повечето случаи.

Може никога да не знаем кой стои зад Octopus скенера, но според изследванията на GitHub той съществува още от 2018 г.

GitHub планира да подобри целостта и сигурността на веригата за доставки на OSS чрез въвеждане на Dependency Graph, предупреждения за сигурност за уязвими зависимости, автоматизирани актуализации на защитата, както и сканиране на код, които помагат да се открият потенциални проблеми в кода ,

Как да проверите дали сте заразени

Продуктите на Sophos идентифицират извадките на зловреден софтуер чрез имената Java / Agent-BERX и Java / Agent-BERZ. Ако сте програмист на NetBeans, можете да търсите тези имена в своите дневници за доказателства за файлове на Octopus скенера в собствената си среда за изграждане на код.

За повече информация:

https://nakedsecurity.sophos.com/2020/06/01/github-uncovers-malicious-scanner-targeting-developers/

Критичните грешки на Exim са поправени, но много сървъри все още са изложени на риск

01 юни 2020 г.

Пачването на пощенските сървъри на Exim не върви достатъчно бързо и членовете на руската хакерска група Sandworm активно експлоатират три критични уязвимости, които позволяват дистанционно изпълнение на отдалечена команда или код.

Понастоящем близо милион Exim сървъри са уязвими, въпреки че броят им постепенно намалява с всеки изминал ден. В момента Exim 4.93 се счита за безопасна версия.

Американската агенция за национална сигурност (NSA) в четвъртък предупреди, че от август миналата година хакерите използват CVE-2019-10149 („Завръщането на WIZard“).

Недостатъкът позволява стартиране на отдалечени команди на сървъри с инсталирани Exim 4.87 до 4.91. Той бе поправен през юни 2019 г.

Изследователи от RiskIQ откриха, че при атаките на Sandworm се използват още две грешки в защитата на Exim сървърите. И двете са критични и могат да бъдат експлоатирани отдалечено без удостоверяване за стартиране на код или на приложения с root права:

CVE-2019-15846 - засяга всички версии на Exim - включително до 4.92.1, докладвана през юли 2019 г. и се появява пач в началото на септември 2019 г.

CVE-2019-16928 - засяга всички Exim сървъри 4.92 до 4.92.2, пач се появява в края на септември 2019 г.

От 1 май изследователите на RiskIQ забелязват в базата данни за интернет разузнаване на компанията, че има повече от 900 000 уязвими сървъра.

Според техните данни организациите са започнали да актуализират своите пощенски сървъри Exim и през последния месец са регистрирани по-малко уязвими версии. Прилагането на пачове обаче е бавно.

Бегъл поглед към Shodan показва малко над милион несвързани Exim (4.92) сървъри онлайн, повечето от тях са в Съединените щати, следвани от Германия и Русия.

NSA предоставя два IP адреса и име на домейн, свързани с дейността на Sandworm, за да помогне на организациите да определят дали са били мишена на атаката.

95.216.13.196

103.94.157.5

hostapp.be

Хакерите са използвали CVE-2019-10149 за изтегляне и изпълнение на скрипт, който им е позволил добавяне на привилегировани потребители, деактивиране на настройките за защита на мрежата, актуализиране на SSH конфигурации, за да се даде възможност за допълнителен отдалечен достъп, изпълнение на допълнителен скрипт за активиране на последваща експлоатация ".

Скриптът предоставя пълен достъп до компрометираните сървъри и всички бази от MySQL, работещи на него. Тук можете да намерите анализ на командите, включени в скрипта на Sandworm.

Какво да предприемете?

Актуализирайте до версия Exim 4.93, която към момента се счита за безопасна.

За повече информация:

https://www.bleepingcomputer.com/news/security/critical-exim-bugs-being-patched-but-many-servers-still-at-risk/