CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 01.04.2020 г.

Съдържание

Marriott International потвърждава за изтичане на данни на до 5,2 милиона гости

31 март 2020

Вегригата хотели Marriott International обяви днес, че е претърпяла изтичане на данни, засягащо до 5,2 милиона души.

Веригата на хотела използва приложение, за да помогне за предоставянето на услуги на своите гости. От средата на януари тази година, идентификационните данни за вход на двама служители във франчайзинг фирма бяха използвани за достъп до информация на гостите на това приложение.

Когато нарушението е открито в края на февруари, Marriott International твърди, че е деактивирала тези идентификационни данни и е започнала разследването си.

Какви данни са били достъпни

• Данни за контакт (име, пощенски адрес, имейл адрес и телефонен номер)

• Информация за акаунт за лоялност (номер на сметката и баланс на точките, но не и пароли)

• Допълнителни лични данни (фирма, пол и ден и месец на рождения ден)

• Партньорства и връзки (свързани програми и номера за лоялност на авиокомпаниите)

• Предпочитания (предпочитания за престой / стая и език)

От Marriott съобщават, че понастоящем няма причина да се смята, че достъпът до информация включва пароли или ПИН кодове за акаунт на Marriott Bonvoy, информация за платежни карти, паспортна информация, национални идентификационни номера или номера на шофьорски книжки.

Marriott е информирала гостите по електронната поща днес (31 март) от адреса marriott@email-marriott.com. В него се съобщава, че се дава възможност на гостите да имат достъп до услуга за наблюдение на данни за една година.

Какво да правя, ако съм засегнат

• Marriott International е създала портал за самообслужване, за да можете да определите дали и каква ваша информация е била достъпна. Също така е посочен

набор от телефонни номера, на които можете да се обадите на страницата му за съобщения за нарушение.

• Ако информацията ви е била замесена, Marriott е деактивирал паролата ви и при следващото влизане ще бъдете подканени да въведете нова. Компанията също препоръчва да активирате двуфакторна автентификация (2FA) в акаунта си, въпреки че не успяхме да намерим тази опцията, когато влезем в системата.

• Бъдете нащрек за измами. Престъпниците обичат да се възползват от подобни изтичания на данни, за да изпращат фишинг имейли или фалшиви уебсайтове. Не кликвайте върху никакви връзки и проверявайте всичко, като се насочвате директно към официалния уебсайт за нарушение или се обаждате на официалните номера на центъра за обаждания. Marriott съобщава, че ако служител на веригата се свърже с вас по имейл, ще го направи от имейл адреса marriott@email-marriott.com и няма да изпраща имейли с прикачени файлове или такива, които искат информация.

За повече информация:

https://nakedsecurity.sophos.com/2020/03/31/marriott-international-confirms-data-breach-of-up-to-5-2-million-guests/

Приложете пач веднага! Критичен недостатък, открит в софтуера за рутери OpenWrt

31 март 2020

Изследовател се натъкна на голям недостатък в сигурността, засягащ OpenWrt, операционна система с отворен код, използвана от милиони домашни и малки бизнес рутери и вградени устройства.

OpenWrt се превърна в популярна Linux алтернатива на фондовия софтуер, който доставчиците доставят с домашни рутери. Други примери за този тип софтуер за рутери включват DD-WRT и Tomato. Може да се използва за замяна на фабричния фърмуер на всеки продукт на рутер с правилния хардуер, например модели от NetGear, Linksys, Zyxel и други.

Открит от Гуидо Вранкен от ForAllSecure, недостатъкът на OpenWrt е в мениджъра на пакети OPKG, програма, използвана за инсталиране или актуализиране на OpenWrt.

За да се гарантира, че тези файлове не са повредени или подправени, преди да бъдат приложени, тяхната цялост се проверява спрямо SHA-256 хеш. Ако двете контролни суми не съвпадат, файлът трябва да бъде изхвърлен.

Въпреки че се обслужват през несигурна HTTP връзка, файловете на OpenWrt са цифрово подписани, което имплицитно гарантира, че посоченият хеш е правилен.

Грешката възниква при стартиране на инсталацията, по време на която Vranken открива, че полето SHA256sum не се чете правилно поради проста грешка в програмирането, нещо, което остава невидимо.

Това означава, че щом атакуващият може да създаде файл, който съответства на посочения размер, той може да вмъкне злонамерен софтуер на рутера или устройството на потребителя, вместо правилния софтуер OpenWrt.

Вранкен предполага, че нападателите могат или да поемат контрол върху сървъра на OpenWrt, или да пречат на DNS на домейна, за да пренасочат потребителите към нелоялен сървър.

Какво да направим

OpenWrt препоръчва ъпдейтване до най-новата версия. Бъгът (CVE-2020-7982) бе представен в началото на 2017 г. и засяга OpenWrt версии 18.06.0 до 18.06.6 и 19.07.0, и отделно LEDE (вилка OpenWrt) 17.01.0 до 17.01.7.

Поправката беше приложена към версии 18.06.7 и 19.07.1, пуснати в началото на февруари.

За повече информация:

https://nakedsecurity.sophos.com/2020/03/31/patch-now-critical-flaw-found-in-openwrt-router-software/

Хакери използват видеоклип с Бил Гейтс, за да продават криптовалутата Ponzi

01 април 2020 г.

Схемата Ponzi се предаваше на живо от следните акаунти в YouTube - Microsoft US, Microsoft Europe, Microsoft News и други.

Наскоро десетки акаунти в YouTube бяха хакнати за излъчване на схема за криптовалути Ponzi, като преименуваха хакнати акаунти в YouTube като акаунти на Microsoft приканващи да инвестирате в криптовалута от бившия изпълнителен директор на компанията Бил Гейтс.

Това не е единствената по рода си атака, различни други атаки като тази станаха чести в YouTube, където хакерът отвлича популярен акаунт и излъчва съобщение от акаунта - „криптовалута“, където на потребителя се дава обещанието, че ако инвестира в някаква криптовалута, ще получи двойна възвръщаемост. Разбира се, това е измама и жертвата не получава никаква възвръщаемост.

Тези измами за пръв път се появиха в Twitter, но се преместиха и в YouTube.

Повечето от измамните видеоклипове се излъчват от хакнати акаунти с голям брой абонати, които са преименувани на Microsoft US, Microsoft Europe и подобни, за да изглеждат по-официални. Гледаният брой на видеоклиповете е в десетки и хиляди, като биткойн адресът в схемата получава хиляди щатски долари, като по този начин успешно мами потребители.

Тези видове измамни схеми вече са доста често срещано явление. Винаги проверявайте легитимността на тези акаунти и е добре да да помислите два пъти, преди да се поддавате на оферта, която е твърде добра, за да е истинска.

За повече информация:

https://www.ehackingnews.com/2020/04/hackers-use-bill-gates-themed-video-to.html