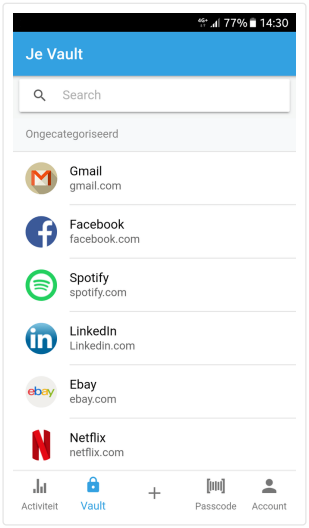
Zoek naar nieuws

Nederlandse wachtwoordmanager Vaulteq stopt ermee

Door **Olaf van Miltenburg**
Nieuwscoördinator
Feedback • 01-02-2019 08:33 • submitter: cHip87

Het Nederlandse bedrijf Vaulteq meldt dat de onderneming opgeheven zal worden. Lopende abonnementen op zijn wachtwoordmanagerdienst stoppen per direct, meldt het bedrijf aan klanten.



Vaulteq meldt dat de ontwikkeling en introductie van de eerste Nederlandse wachtwoordmanager niet tot een winstgevende onderneming heeft geleid. "We zijn daarom genoodzaakt onze onderneming per 28 februari 2019 op te heffen." Abonnementen zijn per direct stopgezet, maar klanten kunnen tot 28 februari hun wachtwoordmanager blijven gebruiken.

Vaulteq biedt de optie voor gebruikers om hun wachtwoorden te exporteren via de optie 'exporteer kluis naar bestand' zodat deze bij een andere manager te importeren zijn. Vaulteq begon in 2016 met het aanbieden van een hardwarematige wachtwoordmanager. Deze 'kluis' was gebaseerd op een Raspberry Pi 2B en moest via ethernet aan een router gehangen worden. In 2017 maakte het bedrijf de overstap naar software. De dienst moest zich onderscheiden met opslag op Nederlandse servers.

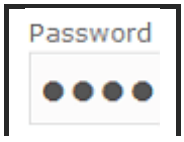
« Vorig nieuwsartikel

Volgend nieuwsartikel »

Lees meer

Gratis wachtwoordmanager Firefox Lockbox is nu ook beschikbaar voor Android

Nieuws van 27 maart 2019



Onderzoek: master password van wachtwoordmanagers is te achterhalen via geheugen

Nieuws van 19 februari 2019

Reacties (107) - Moderatie-faq

Wijzig sortering

107 102 62 6 0 7

Melkunie
1 februari 2019 09:09 • Rapporteer

Zo te lezen ben ik niet de enige die nog nooit van Vaulteq gehoort had.
Daarnaast denk ik ook niet dat ik de enige hier op Tweakers ben met de gedachte "Wachtwoordmanagers, daar moet ik toch echt eens aan beginnen".

Ik zie dat Tweakers hier in 2016 een artikel over gemaakt heeft:
reviews: Datalekkenjaar 2016: kiezen uit wachtwoordmanagers
En een groot topic: [Password Managers] Discussie- en reviewtopic

@Olaf , is het misschien een idee voor een nieuwe round-up op dit gebied?

mcDavid
@Melkunie • 1 februari 2019 12:15 • Rapporteer

Eén ding scheelt, *iedere* passwordmanager is beter dan géén passwordmanager. Je leest een heleboel crud, de één vindt LastPass levensgevaarlijk want cloud, de ander vindt keepass2 veel te ingewikkeld... Uiteindelijk is overal wat voor- en tegen te bedenken, maar zo slecht als zelfbedachte wachtwoorden (proberen te) onthouden voor alle sites waar je ooit hebt ingelogd, is er geen een.

eonflux
@mcDavid • 1 februari 2019 13:59 • Rapporteer

Probeer eens Enpass. Deze gebruik ik, is super eenvoudig, plugin voor in je browser en het allerbelangrijkste. Jij bepaalt waar je vault staat. Onder eigen beheer kan ook via Webdav. De keuze is aan jou. Buy once, use forever.

Ik ben er klaar mee dat elk stukje software een dienst moet zijn waar je voor moet blijven betalen.

Laloeka
@eonflux • 1 februari 2019 16:30 • Rapporteer

En als je een gratis variant wilt:

KeePassXC (een cross(X)-platform Community fork van KeePass) werkt prima als je het combineert met

vullen, al gebruik ik die zelf niet.

[Reactie gewijzigd door Laloeka op 1 februari 2019 16:31]

Dostar

@Melkunie • 1 februari 2019 09:39 • Rapporteer

Helemaal mee eens, en dan ook de afweging tussen: Gratis/Open Source/Betaald en de voor/nadelen van al die pakketten.

Zebby

@Dostar • 1 februari 2019 11:39 • Rapporteer

Heeeeeeeel kort door de bocht vat ik het zo samen:
- maximaal gebruikersgemak: je in-browser keychain (kan ook wachtwoorden genereren en is synced, meestal via een Google of Apple account die weer 2FA zou moeten hebben) of een integratie als Lastpass Gemak en veiligheid! Nadeel is dat het toch in "de cloud" is opgeslagen, en bijvoorbeeld een lastpass wel eens een breuk heeft gehad (zonder gelekte wachtwoorden, maar wel de database). Ook was er een (hele knappe) popup scam die Lastpass echt perfect nabootste.

Voor je gemiddelde gebruiker zou ik altijd die opties aanraden.

- lokale databases: KeePass X of Keepass. Lokaal, dus alleen jij hebt toegang.

Ik zie zelf niet in waarom je voor een betaalde variant zou gaan, maar moet bekennen me er ook niet in verdiept te hebben. Dit is even met focus op particulier, niet zakelijk.

Hoe dan ook, welke je ook kiest, het is beter dan geen wachtwoord manager.

Steef435

@Zebby • 1 februari 2019 12:49 • Rapporteer

Er is ook nog pass. Ontzettend simpel en (dus) makkelijk te integreren in je workflow. Evt ook mogelijk om je store via git (ingebouwd) of iets anders te synchroniseren met je favoriete server. (en de keuze aan "clients" is reuze)

Rascar

@Zebby • 1 februari 2019 13:26 • Rapporteer

Keepass kan je ook synchroniseren met je dropbox. Dit vind ik zelf nog steeds de beste manier.

mcDavid

@Zebby • 1 februari 2019 14:25 • Rapporteer

Een in-browser keychain zou ik niet bepaald becijferen als maximaal gebruiksgemak: je hebt ook passwords die je buiten je browser nodig hebt, hoe doe je dat?

settings geopend te hebben, worden ze veelal gewoon in plain-text opgeslagen.

Zebby

@mcDavid • 1 februari 2019 14:45 • Rapporteer

Tja, anders staan de wachtwoorden hoe dan ook in plain text in een word bestand of zo Heb ik ook te vaak gezien. Gelukkig mijn vader nu over op Keepass die inderdaad zoals @Rascar zegt gesynchroniseerd wordt (maar dan via Stack van TransIP). Zo gebruik ik het zelf zakelijk ook.

Wat betreft de overige wachtwoorden, goed punt, maar ook hier zit je weer met "iets is beter dan niets". Heb je in ieder geval je bankaire en overheidszaken veilig. Ik weet het niet zeker, maar kan me voorstellen dat je in een Lastpass ook zelf wachtwoorden kan toevoegen.

Veiligheid zal nooit zo makkelijk zijn als klakkeloos alles hetzelfde houden. Ergens moet je inleveren. In ieder geval in de huidige markt.

telenut

@Zebby • 1 februari 2019 14:32 • Rapporteer

iemand die van zichzelf nog een password manager gebruikt zou ik niet aanraden een manager te gebruiken die database niet in de cloud opslaat. Het zijn de eerste die er in slagen hun database te verliezen...

Libbz

@Melkunie • 1 februari 2019 09:37 • Rapporteer

Gewoon aan beginnen. Zal je beste beslissing van de laatste jaren voor je zijn. No joke

teek2

1 februari 2019 08:55 • Rapporteer

Ja, toch bizar dat niemand het kent, ik vind het passwoordmanager landschap ook niet optimaal en sta zeker open voor zulke dingen. Ze hadden toch een keer Tweakers moeten inschakelen voor wat reclame...

nst6ldr

@teek2 • 1 februari 2019 09:46 • Rapporteer

> Ze hadden toch een keer Tweakers moeten inschakelen voor wat reclame...

Tweakers heeft een actie gehad waar het apparaat gratis te testen was, en ook zijn ze in het nieuws geweest met hun cloud dienst.

In beide gevallen werden ze niet echt positief onthaald. Het apparaat werd als knullig beschouwd, de cloud dienst werd onthaald met veel scepsis. Al met al hadden ze misschien beter *niet* Tweakers als marketingplatform kunnen gebruiken aangezien men hier wat meer kritisch is wanneer het op security aan komt (al dan niet selectief, want Telegram is schijnbaar weer wél OK).

niet gebruiken voor je wachtwoorden, en een apparaat waarvan alleen toezeggingen bekend zijn doet ook niet veel vertrouwen wekken. Als je daarbij tevens met uitgekauwde marketing termen gooit (military grade!) dan wekt dat zelfs argwaan.

Mocht CT dit nog lezen en een nieuwe poging wagen: maak broncode openbaar, laat onafhankelijke beveiligingsonderzoekers eens los gaan op je apparatuur. Laat hashes zien, leg uit hoeveel moeite er gestoken is in het veilig houden van het product (de procedures, het ontwikkelproces, de inkoop hardware, etc). Dat zijn de dingen die vertrouwen opwekken en je op de kaart zetten.

Anoniem: 167912

@nst6ldr • 1 februari 2019 10:24 • Rapporteer

> Als het op security aan komt wil je compleet open source gaan.

dat hoeft niet per sé, kijk naar apple

Gimmick

@Anoniem: 167912 • 1 februari 2019 12:19 • Rapporteer

> [...]
>
> dat hoeft niet per sé, kijk naar apple

Tja als het niet open is, hoef je niet te bekennen ...
* Facetime-bug, die kennelijk al een keer eerder gemeld was, maar genegeerd
Wat wordt er nog meer 'genegeerd' ?

[Reactie gewijzigd door Gimmick op 1 februari 2019 12:19]

fapkonijntje

@Anoniem: 167912 • 1 februari 2019 12:32 • Rapporteer

Apple is wel een beetje een twijfelgeval. Sommige dingen doen ze zeker goed, ze praten ook vooral heel stoer over privacy en security... Maar daar staat tegenover dat er écht veel fout is gegaan in het verleden en nu nog regelmatig.

Zo zijn lange tijd verwijderde bestanden, notities e.a. jaren later nog op te vragen via icloud. Daarnaast was het ook mogelijk om verwijderde browsegeschiedenis terug te halen. Ook jaren later nog. Waren ze heeel laat met 2FA en dat nog met een zeer gebrekkige implementatie. Nu gelukkig iets beter, maar het begin was dramatisch.

Encryptiekeys van versleutelde schijven in plain text in logfiles, inloggen als root door gewoon je wachtwoord leeg te laten. In plaats van een wachtwoord hint, gewoon het wachtwoord zelf laten zien (wat dus ook betekent dat ergens op je systeem/in je geheugen je wachtwoord plain text beschikbaar is, heel gevaarlijk). Zo zijn er nog wel meer rare dingen. Ook iOS zelf kent de nodige lockscreen bypasses die zo kinderlijk eenvoudig zijn dat ik er zelf wel een beetje van schrok. En ik heb jaren in het appelkamp gezeten, met macbook en iphones.