Faille d’iCloud : Apple avait-il été alerté depuis des mois ?

	Faille d’iCloud : Apple avait-il été alerté depuis des mois ?

Au début du mois, Apple a été sévèrement mis en cause suite au vol et à la publication sur Internet de photos intimes de nombreuses célébrités américaines. La firme a assuré que ses serveurs n'avaient pas été piratés et promis une meilleure protection à l'avenir.

Or selon The Daily Dot, cet incident aurait pu être évité. Comment ? En corrigeant bien plus tôt une faille de sécurité d'iCloud. Car cette vulnérabilité serait celle finalement corrigée fin août. Pourtant, celle-ci aurait été signalée à deux reprises à Apple par un chercheur en sécurité, Ibrahim Balic.

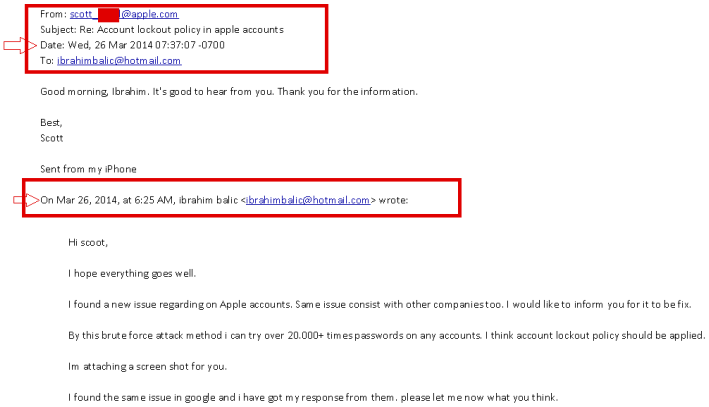
Apple réfute tout lien entre la faille et le vol des photos

Comme l'attestent des emails publiés par le Daily (ci-dessous), l'expert a informé Apple dès le 26 mars d'une méthode permettant d'exécuter une attaque en « brute force » afin de forcer l'accès à un compte iCloud.

Il était en effet possible de tester de très nombreuses combinaisons pour se connecter, Apple n'ayant pas introduit de limitations du nombre de tentatives autorisées. Balic expliquait ainsi avoir pu essayer plus de 20.000 mots de passe.

Début mai, la vulnérabilité ne semblait toujours pas corrigée, l'équipe sécurité d'Apple continuant d'interroger le chercheur sur sa découverte et jugeant par ailleurs la méthode de Balic trop longue pour accéder effectivement de manière illicite à un compte.

Cette faille au niveau de la fonction « Localiser mon iPhone » a-t-elle permis de dérober des photos sur iCloud ? Apple a réfuté tout lien et affirmé que ces divulgations résultaient uniquement d'attaques ciblées contre les victimes.



From : scott_[redacted]@apple.com
Subject: Re: Account lockout policy in apple accounts
Date: Wed, 26 Mar 2014 07:37:07 -0700
To: ibrahimbalic@hotmail.com

Good morning, Ibrahim. It's good to hear from you. Thank you for the information.

Best,
Scott

Sent from my iPhone

On Mar 26, 2014, at 6:25 AM, ibrahim balic <ibrahimbalic@hotmail.com> wrote:

Hi scoot,

I hope everything goes well.

I found a new issue regarding on Apple accounts. Same issue consist with other companies too. I would like to inform you for it to be fix.

By this brute force attack method i can try over 20.000+ times passwords on any accounts. I think account lockout policy should be applied.

Im attaching a screen shot for you.

I found the same issue in google and i have got my response from them. please let me now what you think.

Ibrahim Balic 26-Mar-2014 09:21 PM

Hi Again,

Same issue here:

GET https://p05-mailws.icloud.com:443/wm/ext/sendfrom HTTP/1.1
Host: p05-mailws.icloud.com:443
Connection: keep-alive
Proxy-Connection: keep-alive
Accept: */*
If-Modified-Since: Mon, 24 Mar 2014 00:18:15 Eastern European Standard Time
User-Agent: iPhone Mail (11D167)
Authorization: X-MobileMe-AuthToken base64(userid:password) // MTA[redacted]
Accept-Language: en-us
Accept-Encoding: gzip, deflate

Ibrahim Balic 26-Mar-2014 03:34 PM

Summary:
hi guys,

I found a method for brute-force attack. I found the same issue in google and I've tried 20.474 times password to any account. Account is not locked, malicious people can be exploit here.

"Authorization" parameter in header allowed userid and user password. (with base64 encode)

POST https://p05-keyvalueservice.icloud.com/sync HTTP/1.1
Host: p05-keyvalueservice.icloud.com
Accept: */*
X-Apple-Request-UUID: [redacted]
Authorization: X-MobileMe-AuthToken base64(userid:userpassword)
Content-Encoding: gzip
Proxy-Connection: keep-alive
X-MMe-Client-Info: <iPhone6,1> <iPhone OS;7.1;11D167> <com.apple.SyncedDefaults/166.7>
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-us
X-Apple-Scheduler-ID: com.apple.syncedpreferences
Accept-Encoding: gzip, deflate
User-Agent: SyncedDefaults/166.7 (iPhone OS;7.1 (11D167))
Content-Length: 395
Connection: keep-alive

Steps to Reproduce:

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/faille-d-icloud-apple-avait-il-ete-alerte-depuis-des-mois-39806921.htm
Apple warned of iCloud brute-force vulnerability 6 months before Celebgate