Western Digitali My Cloud salvestusseadmetest avastati sisseehitatud tagauks

7 years tagasi Autor: AM

Kas see on tavaline või jälle kellegi kogemata koodi unustatud näpukas? Kui sul juhtub kasutusel olema Western Digitali My Cloud võrgusalvestusseade ja sa pole selle operatsioonisüsteemi viimasel ajal uuendanud, siis võib sellel olla sisseehitatud tagauks, mille kasutajanimi ja parool on avalikkkusele lekkinud.

Tagaukse kaudu saab sisse logida viimase uuenduseta Western Digitali My Cloud seadmetesse kasutajanimega `mydlinkBRionyg` ning parooliga `abc12345cba`.

Gulftechi töötaja James Bercegay postitas sellel lehel ülevaate mitmetest My Cloudi turva-aukudest ja muuhulgas oli seal avaldatud ka võimalik kood, mida seadmed kasutavad.

```
if (!strcmp(v3, "mydlinkBRionyg") && !strcmp((const char *)&v9, "abc12345cba") ) { result = (struct passwd *)1; }
```

Juhuslik aps? Paljud turvaeksperdid ja häkkerigrupid nii ei arva. Dawid Bałut kirjutab Hackernoonis, et kui see oli ka turva-aps, siis see tähendab, et isegi 19 miljardi dollarise kasumiga ja 77 000 töötajaga megaettevõte on täiesti saamatu oma klientide turvalisuse tagamisel ja laseb oma toodetesse sisse istutada tagaukse, mille kaudu kes teab milline seltskond saab ligipääsu nende klientide kõigile andmetele. Ja need kliendid on heas usus, et nad maksid rohkem tuntud bränditoote eest, sest see tagab turvalisuse.

Tegelikult on olukord veel hullem. On mitmeid näiteid, kus sellised suurfirmad, kes teenivad korralikku kasumit ja keda kliendid usaldavad, vilistavad igasugustele vihjetele oma võimalike turva-aukude kohta. Mõnikord saadetakse võimuorganid "ähvardajat" kimbutama.

James Bercegay teavitas oma avastusest Western Digitali juba 2017. aasta suvel. Peale kuut kuud, mis on piisav aeg, et midagi ette võtta ja rahulikult turva-auk suuremate mainekahjudeta ära parandada, avaldas Bercegay kogu tõe koos tagaukse paroolidega. Jah, veidi inetu tegu, sest tuhanded kasutajad üle maailma jäid kõigi oma andmetega ju seepeale lahtise uksega ja igaüks võis vaadata, kes viitsis.

Tagauksega mudelid on My Cloud Gen 2, My Cloud EX2, My Cloud EX2 Ultra, My Cloud PR2100, My Cloud PR4100, My Cloud EX4, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100 and My Cloud DL4100. Kui tead nende võrguaadressi (IP aadressi või domeeni), siis saab selle kombinatsiooniga juurkasutaja õigused ning teha seadmes, mida ise tahad - kopeerida, kustutada, muuta andmeid või oma skripte sinna istutada.

Kasutajanimes sisalduv *Dlink* vihjab ühele teisele võrgusalvestusseadmete tootjale D-Linkile. Arvatakse, et Western Digital kasutas oma püsivaras sama koodi, mis D-Link DNS-320L ja see sisaldas sama tagaust, mis oli D-Linki seadmel 2014. aastal. D-Link ise kõrvaldas selle turvaaugu üsna ruttu.

Kas minu WD seade on tagauksega?

Praeguseks on Western Digitalil uuendus, mis tagaukse kinni paneb. Selleks, et teada saada, kas sinu seade on ohutu, uuri välja selle püsivara versioon. Vanemad versioonid kui 4.x on tagaukse kaudu sissepääsetavad. Sel juhul tuleb võrgusalvesti kohe avalikust võrgust eraldada ja tarkvarauuendus ära teha.

- Uudised

- Salvestusseadmed
- Turvalisus
- Võrguseadmed

Pilt


BACKDOOR