Asociación de Internautas

Discos duros Western Digital 'My Cloud' tienen una puerta trasera codificada y varios fallos de seguridad adicionales.

Discos duros Western Digital 'My Cloud' tienen una puerta trasera codificada y varios fallos de seguridad adicionales.

Debo ser sincero: estoy empezando a cansarme de todas las vulnerabilidades y fallos de seguridad de la tecnología hoy en día. Francamente, entre Spectre y Meltdown, vehículos conectados a internet sin la mas mínima seguridad, tanques de gasolineras expuestos directamente a internet, la inminente perdida de la neutralidad de la red a nivel mundial, 2018 parece ser el año de las grandes vulnerabilidades y yo me siento desamparado. Hace falta mucha mas concienciación y mas de un tirón de orejas.

Volviendo al tema que nos ocupa, hoy hablamos de otro error de seguridad y es realmente preocupante. Muchas unidades Western Digital My Cloud NAS tienen una puerta trasera codificada, lo que significa que cualquiera puede acceder a ellas; sus archivos podrían estar en riesgo. Usar esta puerta trasera es sumamente facil: el nombre de usuario es "mydlinkBRionyg" y la contraseña es "abc12345cba" (sin comillas). Para empeorar las cosas, se reveló a Western Digital hace seis meses y aparentemente la compañía no hizo nada hasta *noviembre de* 2017. Seamos realistas: no todo el mundo se mantiene al tanto de las actualizaciones, y una puerta trasera nunca debería haber existido en primer lugar. **Echadas las cuentas hablamos de cerca de 180.000 TB de datos de nominas, talones, contabilidades enteras y mas de un video de boda :)**

Adicionalmente otro fallo permite obtener un shell remoto como root y es un proceso bastante trivial que se realiza simplemente publicando un archivo en dichos discos.

Y no acaba allí. Hay otros dos fallos que afectan de forma directa a estos dispositivos:

Uno de ellos permite subir ficheros sin restricción alguna. Esto abre la posibilidad de que un atacante nos pueda infectar el mismo con ficheros maliciosos e incluso chantajearnos posteriormente.

Otro permite lanzar commandos remotamente para resetear configuraciones del mismo de forma remota.

Pero espera: ¿por qué un producto de Western Digital tiene un nombre de usuario codificado que contiene *dlink* ? Raro ¿no? Resulta que los dispositivos WD NAS una vez compartieron el código con los dispositivos D-Link "Sharecenter". Curiosamente, estos equipos D-Link recibieron el firmware parchado en 2014 y ya no contienen la puerta trasera.

WesternDigital tuvo mucho tiempo para arreglar esto. Se le informó en junio del año pasado de estos fallos, pero al parecer, no se hizo nada durante muchos meses.

- 2017-06-10: vendedor contactado a través del formulario de contacto web.Caso asignado # 061117-12088041.

- 2017-06-12: el miembro de soporte Gavin nos refirió a WDC PSIRT. Inmediatamente enviamos una copia encriptada de PGP de nuestro informe a WDC PSIRT.
- 2017-06-13: Recibió la confirmación del informe de Samuel Brown.
- 2017-06-16: el vendedor solicita un período de 90 días hasta la divulgación completa.
- 2017-12-15: Zenofex publica la divulgación del error de carga independientemente de mi investigación
- 2018-01-03: divulgación pública

Si no está seguro de si su dispositivo My Cloud Storage se ve afectado, consulte la lista a continuación. Si su modelo está en la lista, debe desconectarlo de internet inmediatamente.

Aparentemente, el firmware 2.30.165 (emitido en noviembre de 2017) corrige el error, por lo que no debe volver a conectarse a Internet hasta estar seguro de que su dispositivo está actualizado y de que la vulnerabilidad está parchada.

- Mi nube
- MyCloudMirror
- My Cloud Gen 2
- Mi nube PR2100
- Mi nube PR4100
- My Cloud EX2 Ultra
- My Cloud EX2
- Mi nube EX4
- My Cloud EX2100
- My Cloud EX4100
- Mi nube DL2100
- Mi nube DL4100

Incluso si ha actualizado el firmware en noviembre, sus archivos podrían haber sido accedidos durante años por terceros antes de esa fecha.

Articulo de Claudio Chifa basado en el trabajo de investigación de GulfTech, Exploitee.rs

```
[] //hacking_wd_mycloud/
[] /.php?topic=
[] /.php/Western_Digital_MyCloud
[] /
```
