MWR LABS

Security Advisory

LG G3 Arbitrary File Retrieval from Cloud Services

16/01/2017

Product	LG G3/G4/G5
Affected Versions	Smartshare.Cloud < v.2.4.0
CVE Reference	N/A
Author	Masande Mtintsilana
Severity	High
Vendor	LG
Vendor Response	Patch Issued

Description:

LG SmartShare.Cloud is a gateway application provided by LG to access various cloud services such as Dropbox and Box from native applications. A vulnerability was found when an LG device connected to a WiFi network, the SmartShare.Cloud application would start an HTTP Server listening on all interfaces. If an attacker knew the name of a file stored on the Cloud storage, they could retrieve the file without authentication or user interaction.

Impact:

An attacker on the same network as a user who has configured Dropbox or Box as their cloud backup store using LG SmartShare.Cloud application could retrieve any media file from the Cloud storage of the victim as long as they knew the file name.

Cause:

This was due to the SmartShare.Cloud application launching an unauthenticated HTTP Server listening on all interfaces while connected to a WiFi network.

Interim Workaround:

An interim workaround would be to ensure that LG SmartShare.Cloud is not configured to backup local files. Full remediation will require the patch to be applied.

Solution:

Upgrade to the latest version via an OTA (over the air) update. Version 2.4.0 has mitigated this issue.

Technical details

When setting up a cloud backup account, such as Dropbox, the application made available a local HTTP Server on port 9999. This allowed native applications to make requests to backup or retrieve files from the cloud account. However, when the handset was connected to WiFi network, the HTTP Server was made available on all interfaces. The HTTP Server can be queried from another host on the same network to download a known file from the Dropbox account. For example, performing the following GET request from the attacking host will result in the file specified in the file parameter to be downloaded.

```
http://<phone-ip-addr>:9999/?mode=400&account=100000001&file=Getting+Started+with+Dropbox.pdf
```

The SmartShare.Cloud application accepted this request without requiring any authentication. An attacker could scan a network for any devices which have this port open and proceed with the above mentioned attack.

Detailed Timeline

Date	Summary
2016-07-06	Issue reported to LG Product Security Response Team(PSRT)
2016-07-13	LG verifies issue and begins investigation possible fixes
2016-08-03	LG states that issue will be mitigated by checking that source and destination IP addresses are both internal
2016-10-13	LG states that a patch has been released
2016-12-01	LG announces issue in December's Security Bulletin