MWR LABS

Security Advisory

LG SmartShare.Cloud Path Traversal Vulnerability

16/01/2016

Software	Smartshare.Cloud (Cloudhub)
Affected Versions	<V2.4.0
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. The SmartShare.Cloud application started an HTTP Server on all interfaces which allowed users on the same network to issue requests for files stored by the cloud service provider. A Path Traversal vulnerability was found in a URL parameter which allowed an attacker to change the API call being made to Dropbox. If an attacker knew a name of a file or folder stored on Dropbox, it would have been possible to make the file or folder shareable without requiring authentication or user interaction.

Impact:

An attacker on the same network as a user who had configured Dropbox as their cloud backup storage using LG SmartShare.Cloud application could make any media file or folder shareable without authentication or user interaction.

Cause:

This was due to the application not validating that URL parameters did not contain potentially malicious characters.

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

It was found that the SmartShare.Cloud application made available an HTTP Server on port 9999 on a public interface when connected to a WiFi network. This allowed an attacker on the same network to perform requests for arbitrary files stored on the configured cloud service provider. This vulnerability, reported previously, had limitation as an attacker was required to know a name of a file stored by the cloud service provider. Using a path traversal vulnerability, it was possible to change the Dropbox API call being made by SmartShare.Cloud to target a directory or file of the attacker's choosing. This made available API calls to make folder names shareable, increasing the chances of a successful attack as names such as "Pictures" and "Documents" are common for folders.

In the following URL, the file parameter was vulnerable to a path traversal attack.

```
http://10.10.10.5:9999/?mode=200&account=100000001&file= ../../../1/shares/auto/photos
```

Submitting a request with the above URL resulted in the SmartShare.Cloud application issuing a request to the following URL:

```
https://api.dropboxapi.com /1/media/auto/../../../1/shares/auto/photos
```

This resulted in Dropbox interpreting the request as the following URL:

```
https://api.dropboxapi.com/1/shares/auto/photos
```

As a result, instead of requesting for a media file, the specified directory (i.e photos) was made shareable, and a URL link to this resource was returned to the attacker.

Detailed Timeline

Date	Summary
2016-07-06	Issue reported to LG Product Security Response Team(PSRT)
2016-07-13	LG verifies issue and investigates possible fixes

2016-08-03	LG states that issue will be mitigated by encrypting and signing parameters.
2016-10-13	LG states that a patch has been released