Yale Home System (Europe) Man in the Middle Command Execution Vulnerability

24/11/2015

Software:	Yale Home System (Europe) Android Application (yale.webview)
Affected Versions:	<1.11
CVE Reference:	N/A
Author:	MWR Labs (http://labs.mwrinfosecurity.com/)
Severity:	High
Vendor:	Assa Abloy Ltd.
Vendor Response:	Issue resolved and new version released

Description

The Yale Home System (Europe) for Android is part of the Smartphone alarm system. The application allows users to monitor and control their home alarm systems.

A vulnerability was discovered that would allow an attacker to perform a man in the middle attack, bypassing the TLS protection and executing arbitrary commands on the Android device with the permissions of the Home System app.

Impact

If an attacker was able to intercept the communications of a user using the Yale Home System application, then they would be able to read and alter any of the data going to and from the application and the server.

The attacker would also be able to include specific messages to the Android application that would allow them to run commands on the device within the privileges of the Yale Home System application

Cause

The Yale Home System Android application is based upon a Webview. This is a feature of Android that allows applications to display HTML content within their apps.

It was found that the Webview used in the application was configured to ignore TLS errors. This means that if the network traffic was intercepted by an attacker, the application would ignore the security warnings and continue communicating, allowing the attacker to read and alter the communications between the application and the server.

The Webview was also configured to use a JavaScript Interface. There is a known issue with older versions of Webview (compiled with SDK < 17) that means if an attacker can inject their own traffic, then they can use this interface to execute any command they wish on the device with the permissions of the application.

This means that if a user is on the same network as an attacker, or connects to a WiFi hotspot controlled by the attacker, then the attacker would be able to read credentials sent by the user, and run commands on their Android device.

Interim Workaround

The application should not be used on untrusted networks such as public WiFi hotspots.

Solution

All users should update to the latest version of the application. This is version 1.11 at time of publication.

Technical details

It was found in the AndroidManifest.xml that the application was compiled with an old version of the Android SDK:

```
    <uses-sdk android:minSdkVersion="8" android:targetSdkVersion="16" />
```

The WebView used in the application was configured to override the normal security features and ignore TLS errors:

```
class MyWebViewClient extends WebViewClient {
…
public void onReceivedSslError(WebView view, SslErrorHandler handler, SslError error) {
            handler.proceed();
        }
```

Finally a JavascriptInterface was set up on the webview, which given the low SDK version, means that it can be misused, by adding extra Javascript into the messages returned by the server. For example, including the extra line of HTML code in the response from the server would write a file in /data/data/yale.webview/ called mwr.txt:

```
<script>
function execute(cmd){
  return
window.JSInterface.getClass().forName('java.lang.Runtime').getMethod('getRuntime',null).invoke
(null,null).exec(cmd);
}
execute(['/system/bin/sh','-c','echo \"mwr\" > /data/data/yale.webview/mwr.txt']);
</script>
```

Detailed Timeline

Date:	Summary:
01/07/2015	MWR Contact Yale Requested details for sending security details
09/07/2015	Yale provide details for sending security details
10/07/2015	Security details sent
12/10/2015	MWR contact Yale for updates
13/10/2015	Yale respond stating issue is now resolved and update is available from Google Play
24/11/2015	Advisory Published