National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Advisory

The Certifi-gate Vulnerability affects hundreds of millions of Android devices

Original Issue Date: August 28, 2015

Updated: October 06, 2015

Severity Rating: High

Affected Systems:

- Android devices

Description:

Security researchers spotted a new vulnerability known as "Certifi-gate" in Android affecting millions of devices. Certifi-gate is a set of vulnerabilities in the authorization methods between mobile Remote Support Tool (mRST) apps and system-level plugs on a device. mRSTs allow remote personnel to offer customers personalized technical support for their devices by replicating a device's screen and by simulating screen clicks at a remote console. If exploited, Certifi-gate allows malicious applications to gain unrestricted access to a device silently, elevating their privileges to allow access to the user data and perform a variety of actions usually only available to the device owner.

Recently, an application designed to exploit the"Certifi-gate" vulnerability affecting devices running Android has been removed from Google Play. The app known as "Recordable Activator" is an activator for a screen video recording application called Recordable, was downloaded between 100,000 and 500,000 times from Google Play before being removed by Google. As per security experts, the communication with the Recordable Activator component can be spoofed without any authentication, thus allowing any malicious app to record the screen of the device.

Impact of the vulnerability

Security researchers examined the verification methods by which trusted components of the mRSTs validate remote support applications, and discovered numerous faulty exploitable implementations of this logic. This allows mobile platform attackers to masquerade as the original remote supporter with system privileges on the device. This allows an attacker to install malicious applications to gain unrestricted access to a device silently, gain full control of the mobile device including access to the sensitive user and corporate data.

Vulnerable devices
Vulnerable components of these 3rd party mRSTs are often pre-loaded on devices or included as part of a manufacturer or network provider's approved software build for a device. This creates significant difficulty in the patching process and makes affected components impossible to remove or to work around.

Workarounds:
Users are advised to scan their device to determine whether it is vulnerable to Certifi-gate. Security firm Check Point has made available a scanner app, which can be downloaded from Google Play on the following:

https://play.google.com/store/apps/details?id=com.checkpoint.capsulescanner

The following steps are recommended to mitigate the risk:

- Examine carefully any application before installing it to make sure it is legitimate.
- Contact your device manufacturer and mobile carrier to receive information regarding security updates.
- Install the latest version of Android and your ROM as soon as they are issued.
- Uninstall or disable the Remote Support Tool plugs when possible, and according to the vendor's instructions.
- Avoid installing applications from untrusted sources such as 3rd party markets or unfamiliar links.
- Use a mobile security solution to provide protection from malware installed on the device.

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info: contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu