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

Targeted Security Alert

Stagefright 2.0: New vulnerabilities leave a billion Android devices at risk

Original Issue Date: October 05, 2015

Severity Rating: High

Affected Systems:

- Android devices

Description:

Two new Android vulnerabilities, similar to the original "Stagefright" bug have been identified and can allow remote attackers to gain control of vulnerable devices when a victim views a preview of an .mp3 or .mp4 file.

"Stagefright" is a potential exploit that targets the Android operating system. The issue is that a video sent via MMS (text message) could be used as an avenue of attack through the "libStageFright" mechanism (thus the "Stagefright" name), which helps Android process video files. Many text messaging apps automatically process that video which is ready for viewing as soon as a user opens the message, and therefore the attack theoretically could happen without the knowledge of the user.

The two vulnerabilities which reside in "libutils" and in "libstagefright" respectively, can allow for a remote code execution on Android devices, leading to a privilege escalation. These vulnerabilities can grant the attacker complete control of the compromised device. Successful exploitation of the vulnerabilities can allow an attacker with this level of access to install malware and steal information, among other malicious actions.

The attack can be triggered through the following ways:

1. An attacker would try to convince an unsuspecting user to visit a URL pointing at an attacker controlled Web site (e.g., mobile spear-phishing or malicious ad campaign)

2. An attacker on the same network could inject the exploit using common traffic interception techniques (MITM) to unencrypted network traffic destined for the browser.

3. 3rd party apps (Media Players, Instant Messengers, etc.) that are using the vulnerable library

Impact:

- Remote Code Execution (RCE) impact via “libstagefright” on Android 5.0 and later
- Older devices may be impacted if the vulnerable function in “libutils” is used (using third party apps, vendor or carrier functionality pre-loaded to the phone).

Workarounds:

1. Users are advised to proceed cautiously when using their mobile browser to preview unsolicited audio and video files.
2. Android users are advised to apply any security updates issued by their carrier or device manufacturer as and when they become available.

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