Short Term Mitigation for Stagefright Threat on Android		
Device or App Type	**Action**	**User or EMM Console Configured?**
Samsung SAFE devices	Disable incoming MMS on the device	This can be configured in the EMM console as a lockdown policy. This lockdown configuration option is only available on Samsung SAFE devices. Disabling MMS prevents an attacker from sending a malicious MMS message to the user to attempt to exploit the vulnerability.
Google Hangouts App	In Google Hangouts settings, disable "Auto Retrieve MMS"	This action must be done by the user and cannot be done via the EMM console. Prevents the vulnerability from being exploited within Google Hangouts prior to the user viewing the malicious file.
Google Messenger App	In Google Messenger settings, disable "Automatically Retrieve MMS Messages"	This action must be done by the user and cannot be done via the EMM Console. Prevents the vulnerability from being exploited within Google Messenger prior to the user viewing the malicious file.
Android 4.4 devices	In Google Messenger settings, enable "Block Unknown Senders." (option not available on Android 5.0 devices)	This action must be done by the user and cannot be done via the EMM Console. Prevents malicious MMS messages from being received from unknown senders.
Samsung Galaxy S6 devices	Go to "Messages app -> More -> Settings -> More settings -> Multimedia messages -> Auto retrieve." Disable Auto retrieve	This action must be done by the user and cannot be done via the EMM Console. Prevents the vulnerability from being exploited within Samsung Messages app prior to the user viewing the malicious file.