NEWS BRIEF

Android "Stagefright" Bug: What You Need to Know

Security experts at Zimperium identified a major vulnerability in Android's operating system that leaves as many as 95 percent of all Android devices open to attack. Even more frightening—hackers can exploit this vulnerability to gain unfettered remote access to users' phones without users ever knowing.

Stagefright—A Silent Way In

In order for a cyber criminal to gain access to a device, he or she often needs the victim to take some action, like clicking on a link in an email. In the case of the Stagefright bug, the hacker only needs the user's phone number to find a way in.

The vulnerability resides in Stagefright, an Android media playback tool. In order to save the user time, Stagefright "previews" multimedia messages (MMS) so that the user doesn't have to wait as long for something like a video to load.

To exploit the vulnerability, a hacker merely has to embed a malicious code into a video, send the video in an MMS and wait for it to arrive. Even if the user never opens the message, Stagefright's preview tool allows the hacker to gain remote access to the user's phone.

Once a hacker has gained access to the device, there's theoretically no limit to what he or she can do. The hacker could download the user's email or contacts list, hijack the phone's camera and microphone, or even use the phone's GPS to track the user's location.

Patches—Solutions and Problems

The good news is that Google—the company that makes the Android operating system—is aware of the vulnerability and has designed patches to fix the problem. The bad news is Google can't simply send the patch out to the affected users.

Unlike Apple, which provides updates for its operating systems directly to customers who purchase its hardware, Google relies upon device manufacturers, and sometimes phone carriers, to provide users with updates. Making matters more complicated, those manufacturers and carriers also modify the operating systems. So even with Google's patches, it might take even more time to make sure the patch works on each particular device and for each cellphone carrier.

What Comes Next

Device manufacturers and carriers are currently busy working on the problem—according to their own timetables.

However, the best thing **you** can do is be proactive. Check for and install any updates on your device, and find out when your device's manufacturer and your carrier will be issuing patches.

For now, simply be aware that the risk is out there, and your trusted advisor at The Alpha Group will inform you of any new risks to you and your business.

The Alpha Group