Weekly Metasploit Update: Android WebView Exploit

转载

Android WebView Exploit, 70% Devices Vulnerable

This week, the biggest news I think we have is the release this week of Joe Vennix and Josh @jduck Drake's h

Seriously, though, this vulnerability is kind of a huge deal. I'm hopeful that by publishing an E-Z-2-
Use Metasploit module that exploits it, we can maybe push some vendors toward ensuring that single-
click vulnerabilities like this don't last for 93+ weeks in the wild. Don't believe me that this thing is that old? Just

It should be noted that the bug only ("only," he says!) affects versions of Android below 4.2 (early Jellybean). In
contract rack at a couple big-
box stores, and every one that I saw were vulnerable out of the box. And yes, that's here in the U.S., not some f
away place like Moscow, Russia. This lines up with what Android Central reports, in that while Android 4.4 (Kitk

There's a lot more to say here, so expect more on this in the coming days. We've slapped together a quick vide

As you can see, the attack shown here -- QR code on a Metasploit exploit -
- is a pretty dang effective way to get a shell on a target Android device, assuming your QR marketing skills are

Incidentally, who do you lean on to get this patched? The big box retailer who sold it to you? The manufacturer

Mass Check!

Item two on this week's release is Wei @_sinn3r Chen's rework of how Metasploit exploits use the "check" func
- really, go read it, it's good. I'll wait.

Now that you've got the background and it's out in this week's release, you no longer need to guess at how mar scope Windows machines really are vulnerable to MS08-
067 before you try to tag them. This is not to say that Metasploit is suddenly a proper vulnerability scanner. We to-day vuln scanning duties.

Meterpreter Clipboard Monitor

Also on this release (dang, this is a pretty good one this week), is the new clipboard monitor functionality for Me erasing protections of KeePass are completely obliterated.

This makes me sad, as I'm an avid KeepassX user and have been for years and years. Oh well, I guess I just be and-baby pictures.

But, alas, moving security forward isn't just about me and what software I use. The fact of the matter is, passwo based password manager and hope nothing's watching your clipboard, c) use some hand-
typing system of password management and hope you're not getting your keystrokes logged, or d) use a brows based autofill system and hope you're not a recent victim of a universal, persistent XSS bug. Time to take anotl factor authentication (2FA) choices.

Incidentally, we'll have more on the UXSS thing in the next couple weeks. You're welcome, in advance.

New Modules

Including the WebView exploit the above, we're shipping six new exploits and seven new auxiliary and post moc media-in-a-box offering, all from the cruelly-named Kicks4Kittens.

Exploit modules

- Android Browser and WebView addJavascriptInterface Code Execution by joev and jduck
- Kloxo SQL Injection and Remote Code Execution by juan vazquez and Unknown
- Pandora FMS Remote Code Execution by xistence
- KingScada kxClientDownload.ocx ActiveX Remote Code Execution by juan vazquez and Andrea Micalizzi e 14-011
- Windows TrackPopupMenuEx Win32k NULL Page by Dan Zentner, Matias Soler, Seth Gibson, and Spenc 2013-3881
- Windows Command Shell Upgrade (Powershell) by Ben Campbell

Auxiliary and post modules

- IBM Lotus Sametime WebPlayer DoS by Chris John Riley and kicks4kittens exploits CVE-2013-3986
- DoliWamp 'jqueryFileTree.php' Traversal Gather Credentials by Brendan Coles
- IBM Lotus Notes Sametime User Enumeration by kicks4kittens
- IBM Lotus Notes Sametime Room Name Bruteforce by kicks4kittens
- IBM Lotus Sametime Version Enumeration by kicks4kittens
- A10 Networks AX Loadbalancer Directory Traversal by xistence exploits OSVDB-102657
- Windows Gather Active Directory User Comments by Ben Campbell

If you're new to Metasploit, you can get started by downloading Metasploit for Linux or Windows. If you're alread edge of Metasploit development, then these modules are but an msfupdate command away. For readers who p

For additional details on what's changed and what's current, please see Brandont's most excellent release note

转载于:https://blog.51cto.com/xpt51/1387319