Project Zero hunts Galaxy, Samsung responds with eight fixes

November 5 2015, by Nancy Owano

Any Android-vulnerability found in popular smartphones and reported in the press naturally gets everyone looking in Google's direction. What's wrong with those Android engineers?

The situation is not that simple. Most Android devices are not made by Google, but by OEMs (original equipment manufacturers). Android may be the basis but additional code introduced may be vulnerable. What is

more, the OEMs decide on the frequency of security updates provided for their devices to carriers.

A study by the University of Cambridge in October found over half of Android devices as insecure and the study similarly pointed to a difficulty because of some OEMS' lack of updates. The study ranked Nexus devices as the most secure.

"With 87 percent of devices flagged as insecure on any given day, the study really shows how far the Android ecosystem has to go to protect its users," wrote Ron Amadeo in *ArsTechnica*. "Google and some OEMs have committed to a monthly security update program, but that is usually for devices that are less than two years old (Google recently bumped Nexus devices to three years) and only for flagship devices. The vast majority of Android sales are not flagship devices. Until Google re-architects Android to support centralized, device-agnostic updates, we just don't see a solution to Android's security problems."

Vlad Savov in *The Verge* concisely echoed a concern about Android: "Google doesn't control the final software that most people use and experience, and it doesn't have the means to secure each of the 1.4 billion Android devices in active use today."

Natalie Silvanovich of the Project Zero team at Google with the task of hunting out previously unknown computer security flaws, blogged about the team's recent findings. Project Zero's team members had gone on a bug hunt recently using Samsung's Galaxy S6 Edge phone.

Why the hunt? Silvanovich said they had already gone through their own Nexus devices; now they wanted to see how different attacking an OEM device would be.

The rest made this week's news: They found 11 issues needing attention.

The reason they went after the Galaxy phone was not out of assessing that this was a buggy brand and model but because it is a high-end phone which has a large number of users.

Hot Hardware described how they carried out their plan: they gave themselves a week to root out vulnerabilities. They even made a contest out of it. North American participants competed with participants from Europe.

They worked on challenges such as: Gain remote access to contacts, photos and messages; gain access to contacts, photos, geolocation, etc. from an application installed from Play with no permissions; persist code execution across a device wipe.

"Their efforts resulted in the discovery of 11 vulnerabilities," said *Hot Hardware*.

Besides seeing what kinds of bugs they would find, they were also eager to see how quickly bugs would be resolved when they reported them.

Silvanovich said the team reported the issues to Samsung and Samsung responded, stating that they fixed eight of the issues in their October Maintenance Release, and the remaining issues are to be fixed this month. "We greatly appreciate their efforts in patching these issues," she stated.'

As for the three remaining issues to be fixed this month, she said that "Fortunately, these appear to be lower severity issues."

All in all, yes, they found issues in their bug-hunting expedition and, to answer their question about OEM response times, yes, Samsung is a company that responded promptly. "It is promising that the highest severity issues were fixed and updated on-device in a reasonable time

frame," she said.

Samsung, reported *Hot Hardware*, "rolled out fixes for eight of the 11 vulnerabilities, which Project Zero confirmed by re-testing an updated Galaxy S6 Edge."

Reader reactions on *Hot Hardware* included posts expressing satisfaction for a timely response. "Pretty fast action there, of course it is expected in flagship higher end phones."

Another reader response was, "This collective effort is refreshing and users can only benefit from more secure computing. People with older devices should be given incentive to update to newer devices."

More information: googleprojectzero.blogspot.co. … bugs-in-samsung.html

Citation: Project Zero hunts Galaxy, Samsung responds with eight fixes (2015, November 5) retrieved 16 April 2024 from https://techxplore.com/news/2015-11-galaxy-samsung.html