Developer tells Google about Chrome browser listening risk

January 23 2014, by Nancy Owano

(Phys.org) —One developer's posting this week about Chrome has drawn a bunch of headlines from tech sites launching into reports on the developer's headline post: "Chrome Bugs Allow Sites to Listen to Your Private Conversations." Tal Ater, who maintains a JavaScript speech recognition library, annyang, said he made the discovery some months ago while working on annyang. When you click the microphone icon on the right side of the search box, you can enable voice actions where you can speak into the Chrome browser to search, get directions, send messages or any other such basic task. According to Ater, by exploiting

Chrome bugs, malicious sites could turn Google Chrome into a listening device, which could record anything you said in your surroundings as long as Chrome is still running.

"The site asks the user for permission to use his mic, the user accepts, and can now control the site with his voice. Chrome shows a clear indication in the browser that speech recognition is on, and once the user turns it off, or leaves that site, Chrome stops listening. So far, so good," he wrote. "But what if that site is run by someone with malicious intentions?"

In his post this week, he stated: "When you click the button to start or stop the speech recognition on the site, what you won't notice is that the site may have also opened another hidden popunder window. This window can wait until the main site is closed, and then start listening in without asking for permission. This can be done in a window that you never saw, never interacted with, and probably didn't even know was there."

Ater made the discovery in September, and, he said, "wanting speech recognition to succeed, I of course decided to do the right thing." He notified the Google security team in private on September 13. By September 24, he said, a patch which fixes the exploit was ready. "Google's engineers, who've proven themselves to be just as talented as I imagined, were able to identify the problem and fix it in less than two weeks from my initial report." End of story? Apparently, no.

But then time passed, he wrote, and the fix didn't make it to users' desktops. "A month and a half later, I asked the team why the fix wasn't released. Their answer was that there was an ongoing discussion within the Standards group, to agree on the correct behavior."

As of this week, Ater wrote in his post, "almost four months after

learning about this issue, Google is still waiting for the Standards group to agree on the best course of action, and your browser is still vulnerable."

A Google spokesperson reached for comment by sites such as *The Verge* and *Ars Technica*, however, said, "We've re-investigated and still believe there is no immediate threat, since a user must first enable speech recognition for each site that requests it. The feature is in compliance with the current W3C standard, and we continue to work on improvements.".

As for Ater, he said "as the maintainer of a popular speech recognition library, it may seem that I shot myself in the foot by exposing this. But I have no doubt that by exposing this, we can ensure that these issues will be resolved soon, and we can all go back to feeling very silly talking to our computers… A year from now, it will feel as natural as any of the other wonders of this age."

More information: talater.com/chrome-is-listening/