Researcher finds over 300,000 servers still Heartbleed-vulnerable

June 23 2014, by Nancy Owano

Credit: Victorgrigas/Wikideia/ CC BY-SA 3.0

Back in April, discoveries made headlines over a vulnerability in OpenSSL known as Heartbleed. The flaw in OpenSSL, a software library for the protection and security of websites, was uncovered and reported it to the OpenSSL team, triggering widespread awareness and advice on what steps administrators and Web users can take. In June, one can well ask, how are we doing? The answer, according to a security expert tracking the issue, is that many servers remain unpatched and vulnerable. Over half the Heartbleed vulnerable servers are still exposed; at least 309,197 servers are still vulnerable to the exploit; they run unpatched.

Robert Graham, security researcher of Errata Security, released those numbers in a blog on Saturday. At the time of the Heartbleed announcement in April, he said there were 600,000 systems vulnerable to Heartbleed. In May, he found that half had been patched; 300,000 were vulnerable. "Last night, now slightly over two months after Heartbleed, we scanned again, and found 300k (309,197) still vulnerable. This is done by simply scanning on port 443, I haven't check [sic] other ports."

Those numbers indicated to Graham that "people have stopped even trying to patch. We should see a slow decrease over the next decade as older systems are slowly replaced. Even a decade from now, though, I still expect to find thousands of systems, including critical ones, still vulnerable." He said he will scan again in July and also at the six-month mark, then yearly, to track progress.

Following the news of Heartbleed in April, users generally were told that as a safety measure they might choose to use a different password everywhere instead of a blanket password for numerous sites they access and to avoid older, less maintained sites that may not have patched Heartbleed. System administrators were advised to update versions of SSL and to revoke compromised keys and reissue new keys.

Placing the Heartbleed events in perspective, Greg Kumparak, mobile editor at TechCrunch, said on Sunday that "There's a really good reason why security researchers were so spooked by the Heartbleed bug: there's just no silver bullet. Even if we somehow banded together to get most of the world's systems patched, a big chunk of the Internet would likely be left vulnerable. Sure enough, Heartbleed beats on."

More information: blog.erratasec.com/2014/06/300 … wo.html#.U6dgO_kZMhb

Citation: Researcher finds over 300,000 servers still Heartbleed-vulnerable (2014, June 23) retrieved 28 April 2024 from https://techxplore.com/news/2014-06-servers-heartbleed-vulnerable.html