Cybersecurity experts discover lapses in Heartbleed bug fix

November 7 2014, by Andrew Snadecki

A detailed analysis by cybersecurity experts from the University of Maryland found that website administrators nationwide tasked with patching security holes exploited by the Heartbleed bug may not have done enough.

First disclosed in April 2014, Heartbleed presents a serious vulnerability to the popular OpenSSL (Secure Sockets Layer) software, allowing anyone on the Internet to read the memory of systems that are compromised by the malicious bug.

Assistant Research Scientist Dave Levin and Assistant Professor of Electrical and Computer Engineering Tudor Dumitras were part of a team that analyzed the most popular websites in the United States—more than one million sites were examined—to better understand the extent to which systems administrators followed specific protocols to fix the problem.

Levin and Dumitras both have appointments in the Maryland Cybersecurity Center, one of 16 centers and labs in the University of Maryland Institute for Advanced Computer Studies.

Their team, which included researchers from Northeastern University and Stanford University, discovered that while approximately 93 percent of the websites analyzed had patched their software correctly within three weeks of Heartbleed being announced, only 13 percent followed up with other security measures needed to make the systems completely

secure.

Once Heartbleed was made public, Levin says, website administrators everywhere should have immediately taken three steps to regain better control and security over their systems.

"They needed to patch their OpenSSL software, they needed to revoke their current certificates, and they needed to reissue new ones," he says.

Patching, revoking and reissuing are elements of the PKI, or Public Key Infrastructure, which allows for browsers and operating systems to verify that they are communicating with an authentic website, rather than an attacker who is masquerading as a website in order to gain sensitive user information.

But without following through with both revocation and reissue, attackers who already had a website's private key could still pose as that website, even if the administrator had correctly patched their software.

"Many people seem to think that if they reissue a certificate, it fixes the problem, but, actually, the attack remains possible just as it did before. So, you need to both reissue and revoke the certificates," says Dumitras.

The team's data analysis also highlighted an interesting trend that points to the role that humans play in these complex security systems, Dumitras says. In a graph displaying how many certifications were revoked over the course of the three weeks, their data shows a significant drop in revocation rates during weekends.

"Basically, that means that security was taking the weekends off," he says.

Dumitras and Levin hope that the team's findings—presented this week

at the 2014 Internet Measurement Conference in Vancouver, B.C.—will spur conversations regarding the multiple factors that influence overall computer security, and how those factors can work together to better strengthen systems.

"Security isn't something to be taken for granted," Levin says. "I see some of these results and I'm shocked and I'm surprised and I'm a little bit scared. But at the same time, I see it as opportunity for improvement."

More information: Paper link: www.umiacs.umd.edu/~tdumitra/papers/IMC-2014.pdf

Provided by University of Maryland