# 'Heartbleed' fix may slow Web performance

April 15 2014, by Rob Lever

The heartache from the Heartbleed Internet flaw is not over, and some experts say the fix may lead to online disruption and confusion

The heartache from the Heartbleed Internet flaw is not over, and some experts say the fix may lead to online disruption and confusion.

The good news is that most sites deemed vulnerable have patched their systems or are in the process of doing so.

The bad news is that Web browsers may be overloaded by the overhaul

of security certificates, leading to error messages and impacting Web performance, said Johannes Ullrich of the SANS Internet Storm Center.

"A good percentage of the websites are patched," Ullrich told AFP.

The patches enable the Web operators to obtain new security certificates that demonstrate they can be trusted by Web browsers.

But Ullrich noted that for each patch, Web browsers must update their list of "untrusted" certificates or "keys" that would be rejected.

"For the fix, the website needs to obtain a new private key and the old key has to be revoked," he said. "Browsers will not trust the old keys."

Browsers may usually update dozens of keys on a daily basis, but because of Heartbleed, that may rise to tens of thousands.

If the verification process takes too long, Ullrich said, the browser may simply declare the site invalid or show an error message.

"People will see errors," he said. "They will see an invalid certificate. They can either accept the certificate or consider it invalid."

The big danger is that Internet users may become so confused or frustrated that they ignore the warnings or reconfigure their browsers to no longer perform the security check.

"If people turn off those lists, then a hacker could get in," Ullrich said.

With thousands of websites seeking new security credentials, "some certificate authorities and website administrators have been making careless mistakes," online security firm Netcraft noted.

Warnings about the danger have grown over the past week, with everyone from website operators and bank officials to Internet surfers and workers who telecommute being told their data could be in danger.

The bug is a flaw in the OpenSSL encryption at "https" websites that Internet users have been taught to trust.

The Heartbleed flaw lets hackers snatch packets of data from working memory in computers, creating the potential for them to steal passwords, encryption keys or other valuable information.

The security firm Cloudflare reported last week that it appeared impossible to use Heartbleed to steal certificates to impersonate a website, but then reversed itself after a "challenge" to the security community brought out evidence these thefts were possible.

Google said that some versions of its Android mobile operating system may be vulnerable to Heartbleed. On Monday, it urged developers to create new security keys to ensure apps and other services can be trusted.

Trend Micro security specialist Veo Zhang said the latest evidence shows mobile phones are potentially vulnerable in two ways:

"This is because mobile apps may connect to servers affected by the bug," Zhang said in a blog.

"However, it appears that mobile apps themselves could be vulnerable... We have found 273 in Google Play which are bundled with the standalone affected OpenSSL library, which means those apps can be compromised in any device."

Some of the first evidence of hackers using Heartbleed have begun to surface in recent days.

British parenting website Mumsnet announced Monday that users' data had been accessed, potentially compromising 1.5 million accounts.

Officials in Ottawa said personal data for as many as 900 Canadian taxpayers was stolen after being made vulnerable by the "Heartbleed" bug.

The Canadian Revenue Agency last week shuttered its website over concerns about the Heartbleed bug.