'Heartbleed' bug a critical Internet illness

April 11 2014, by Glenn Chapman

In this file photo, a student from an engineering school attends the first edition of the Steria Hacking Challenge, in France, on March 16, 2013

The "Heartbleed" flaw in Internet security is as critical as the name implies and wider spread than first believed. Warnings about the danger exposed early this week reached widening circles on Thursday, with everyone from website operators and bank officials to Internet surfers and workers who tele-commute being told their data could be in danger.

"Heartbleed is a catastrophic bug in OpenSSL," well-known computer

security specialist Bruce Schneier said in a post at his schneier.com website.

OpenSSL is a commonly used software platform for encrypted transactions 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.

"This is going to be a pretty devastating bug," Trustwave security research manager John Miller told AFP.

"Even after the majority of it is fixed on the Internet, there will be internal services vulnerable."

Threat widens

The Heartbleed flaw can be found in virtual private network (VPN) software commonly used by workers on the go to securely link with company computer networks.

Computer networking titans Cisco and Juniper put out advisories on Thursday that some of their data-handling gear is susceptible to the bug.

"An exploit could allow the attacker to disclose a limited portion of memory from a connected client or server," California-based Cisco said in an advisory note.

"The disclosed portions of memory could contain sensitive information."

Canada's tax agency shuttered its website Wednesday after warning that

encrypted taxpayer data could be vulnerable.

A general view of the Cisco booth at the International CES, at the Las Vegas Convention Center in Nevada, on January 7, 2014

OpenSSL is commonly used to protect passwords, credit card numbers and other data sent via the Internet.

Web masters have been scrambling to update to safe versions of OpenSSL. The vulnerability has existed for about two years, since the version of OpenSSL at issue was released.

The Tor Project devoted to letting people use the Internet anonymously advised those in need of privacy to stay offline until the Heartbleed threat is ameliorated.

Crown jewels at risk

Information considered at risk includes source codes, passwords, and "keys" that could be used to impersonate websites or unlock encrypted data.

"These are the crown jewels, the encryption keys themselves," said a heartbleed.com website devoted to details of the vulnerability.

"Leaked secret keys allows the attacker to decrypt any past and future traffic to the protected services and to impersonate the service at will."

The flaw in OpenSSL allows a hacker to read the memory of a machine working the software, but no more than 64 kilobytes of data at a time, according to security specialists.

However, hackers could repeatedly grab packets of memory to ramp up the odds of stealing valuable data.

"We don't know how actively Heartbleed was exploited before publication of the vulnerability," Trustwave's Miller told AFP.

"Since Monday, when they published, it has been used a lot. People have been executing the attack all over the Internet."

In this file photo, a stand offering security solutions for the internet is seen at the CeBIT computer technology trade fair in Hanover, central Germany, on March 10, 2014

OpenSSL is used by more than half of websites, but not all versions have the vulnerability, according to heartbleed.com.

The group behind open-source OpenSSL is urging users to upgrade to an improved version of the software and gave credit for finding the bug to Neel Mehta of Google Security.

Major websites and services were given advanced word of the Heartbleed flaw to allow time for patches to be put in place before the flaw was made public.

Miller and other security specialists said Heartbleed appeared to be the

result of a mistake in writing the OpenSSL code.

Software patches and updates were being rushed out, but it was expected to take time for websites, businesses, router makers and others on the growing list of those at risk to replace software keys used to prevent impersonation or safeguard encrypted data.

Websites need to change credentials used to verify authenticity in order to prevent hackers who may have looted the data from impersonating legitimate online venues and tricking visitors to enter valuable personal information.

Internet users were advised to change passwords to online accounts or services, but only after checking to make sure the Heartbleed flaw has been fixed and new certificates of online identity installed.

While Heartbleed has shaken trust in the Internet, it may well wind up providing insight into which websites or services deserve to be trusted.

"I don't think its a matter of losing faith," Miller said.

"It is really going to be an individual measure of how organizations respond; and we can start to judge their security postures."