# NSA denies exploiting 'Heartbleed' vulnerability

April 11 2014, by Rob Lever



A student from an engineering school attends the first edition of the Steria Hacking Challenge, in France, on March 16, 2013

The US National Security Agency on Friday denied a report claiming it was aware of and even exploited the "Heartbleed" online security flaw to gather critical intelligence.

The stern denial came amid growing panic among Internet users the

world over about the newly exposed flaw, after a report by Bloomberg News said the spy agency decided to keep quiet about the matter and even used it to scoop up more data, including passwords.

"NSA was not aware of the recently identified vulnerability in OpenSSL, the so-called Heartbleed vulnerability, until it was made public in a private-sector cybersecurity report," NSA spokeswoman Vanee Vines said in an email.

"Reports that say otherwise are wrong."

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

A White House official also denied that any US agency was aware of the bug before it was revealed by security researchers earlier this month.

"Reports that NSA or any other part of the government were aware of the so-called Heartbleed vulnerability before April 2014 are wrong," White House national security spokeswoman Caitlin Hayden said in a statement.

"This administration takes seriously its responsibility to help maintain an open, interoperable, secure and reliable Internet.

"If the federal government, including the intelligence community, had discovered this vulnerability prior to last week, it would have been disclosed to the community responsible for OpenSSL."

## 'Part of NSA arsenal'

Bloomberg, citing two people said to be familiar with the matter, said the NSA was able to make Heartbleed part of its "arsenal" to obtain

passwords and other data, without making public a [vulnerability](#) which could affect millions of Internet users.

The report said the secretive intelligence agency has more than 1,000 experts devoted to ferreting out these kinds of flaws and found the Heartbleed glitch shortly after its introduction.

The agency then made it part of its "toolkit for stealing account passwords and other common tasks," the report said.

The claim was met with concerns in the security community.

"If the NSA really knew about Heartbleed, they have some *serious* explaining to do," cryptographer Matthew Green said on Twitter.

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.

Warnings about the dangers have expanded in recent days, with everyone from website operators and bank officials to Internet surfers and workers who tele-commute being told their data could be in danger.

NSA was already in the spotlight after months of revelations about its vast data-gathering capabilities, along with partner intelligence agencies.

Documents leaked by former NSA contractor Edward Snowden indicated that the NSA has been able to collect data from millions of phone records and Internet conversations as part of its intelligence gathering.

NSA officials argue they use such data only to help root out suspected terrorists.

President Barack Obama has ordered reforms that would halt government bulk collection of telephone records, but critics argue this does not go far enough to protect civil liberties.