Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years; NSA Denies Allegations

Image: Codenomicon

Source: Wired.com

Wired.com Update: The NSA has issued a statement denying any knowledge of Heartbleed prior to its public disclosure this week. “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,” an NSA spokesperson wrote in a statement. “Reports that say otherwise are wrong.”

The White House National Security Council spokesperson Caitlin Hayden also denied that federal agencies knew about the bug. “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,” Caitlin Hayden said in a statement.

Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years

The NSA knew about and exploited the Heartbleed vulnerability for two years before it was publicly exposed this week, and used it to steal account passwords and other data, according to a news report.

Speculation had been rampant this week that the spy agency might have known about the critical flaw in OpenSSL that would allow hackers to siphon passwords, email content and other data from the memory of vulnerable web servers and other systems using the important encryption protocol.

That speculation appears to be confirmed by two unnamed sources who told Bloomberg that the NSA discovered the flaw shortly after it was accidentally introduced into OpenSSl in 2012 by a programmer.

The flaw "became a basic part of the agency's toolkit for stealing account passwords and other common tasks," the publication reports. [See NSA response above]

OpenSSL is used by many websites and systems to encrypt traffic. The vulnerability doesn't lie in the encryption itself, but in how the encrypted connection between a website and your computer is handled. On a scale of one to 10, cryptographer Bruce Schneier ranks the flaw an 11.

The flaw is critical because it's at the core of SSL, the encryption protocol so many have trusted to protect their data, and can be used by hackers to steal usernames and passwords – for sensitive services like banking, ecommerce, and web-based email.

There are also concerns that the flaw can be used to steal the private keys that vulnerable web sites use to encrypt traffic to them, which would make it possible for the NSA or other spy

agencies to decipher encrypted data in some cases and to impersonate legitimate web sites in order to conduct a man-in-the-middle attack and trick users into revealing passwords and other sensitive data to fake web sites they control.

Heartbleed allows an attacker to craft a query to vulnerable web sites that tricks the web server into leaking up to 64kb of data from the system's memory. The data that's returned is random – whatever is in the memory at the time – and requires an attacker to query multiple times to collect a lot of data. But this means that any passwords, spreadsheets, email, credit card numbers or other data that's in the memory at the time of the query could be siphoned. Although the amount of data that can be siphoned in one query is small, there's no limit to the number of queries an attacker can make, allowing them to collect a lot of data over time.

Read the rest of the article at Wired.com