

Cybersecurity: Department of Homeland Security Admits that US Government Knew about the Heartbleed Computer Bug?

Why Were Government Computers Immune to the Bug?

By [Washington's Blog](#)

Global Research, April 14, 2014

[Washington's Blog](#)

Region: [USA](#)

Theme: [Intelligence](#)

Bloomberg reported that the [NSA knew about - and exploited -](#) the Heartbleed bug for years.

The NSA has [denied](#) it knew about the bug.

And the White House spokesman [claims](#):

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.

(OpenSSL is the library infected by Heartbleed.)

But the Department of Homeland Security [says](#):

The Federal government's core citizen-facing websites are not exposed to risks from this cybersecurity threat.

Matt Stoller [tweets](#):

DHS says #Heartbleed didn't affect government websites. That is... peculiar.

Perhaps there is an innocent explanation ... The government doesn't use OpenSSL on its websites?

Nope ... Security firm Codenomicon - which discovered the Heartbleed virus - [reports](#):

You are likely to be affected either directly or indirectly. OpenSSL is the most popular open source cryptographic library and TLS (transport layer security)

implementation used to encrypt traffic on the Internet. Your popular social site, your company's site, commercial site, hobby site, sites you install software from or even sites run by your government might be using vulnerable OpenSSL.

Did DHS just unintentionally admit that the government knew about Heartbleed years ago and patched its own websites ... without telling the tech community about it?

Mother Jones [points out](#) that – whether or not the NSA knew about the bug – the Heartbleed episode makes it look bad:

I'm honestly not sure which would be worse. That the NSA knew about this massive bug that threatened havoc for millions of Americans and did nothing about it for two years. Or that the NSA's vaunted—and lavishly funded—cybersecurity team was completely in the dark about a gaping and highly-exploitable hole in the operational security of the internet for two years. It's frankly hard to see any way the NSA comes out of this episode looking good.

The original source of this article is [Washington's Blog](#)
Copyright © [Washington's Blog](#), [Washington's Blog](#), 2014

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Washington's Blog](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca