Heartbleed security bug compromises vast portion of Internet traffic

Joseph Santolan
11 April 2014

On April 7, security researchers announced that they had discovered a significant flaw in OpenSSL, the program responsible for the encryption of a majority of the traffic on the Internet. This vulnerability is being referred to as Heartbleed.

Two-thirds of servers on the Internet use OpenSSL. Not all of the servers that use OpenSSL are affected, however, only those sites which use versions 1.0.1 and later. It is nonetheless likely that a majority of the traffic on the Internet has been affected by Heartbleed.

The Heartbleed bug, whose discovery was announced at the beginning of the week, has been in existence since February 2012. Any individual or organization that discovered the existence of the bug over the past two years would have unfettered access to a vast portion of the private data transmitted across the Internet.

Prominent security expert Bruce Schneier referred to Heartbleed as a "catastrophic bug," stating, "On the scale of 1 to 10, this is an 11."

The scope of the data that has been potentially compromised is astronomical and includes usernames, passwords, bank account and credit card numbers, medical data, documents in online cloud storage.

Not only has all of this user data been directly compromised, but, what is worse, the private keys of the servers running the vulnerable versions of OpenSSL were also almost certainly compromised. These keys are used both for generating the certificates that securely identify a web site to its visitors as well as for decrypting the traffic which is sent to these web sites.

Anyone who was able to obtain these keys would be able to spoof the web site, tricking visiting Internet browsers into treating a fake site set up for malicious purposes as the correct site. Having the private key would also allow all archived past traffic with that server that had been encrypted to that key to be decrypted, even communications that occurred years prior to the introduction of the Heartbleed bug.

Client-side encryption, in which the keys for encryption are controlled not by the server but by the local user, was not affected by Heartbleed. The PGP/GPG encryption protocol for email, the ZRTP encryption of voice communications, such as that used in programs like Jitsi, as well as the OTR protocol for the encryption of chat and text messages, were not affected by Heartbleed.

On the day of the announcement, OpenSSL released version 1.01g which patched the Heartbleed vulnerability. This did not, however, resolve the problem, as every vulnerable server is individually responsible for upgrading OpenSSL to the patched version of the program as well as generating new private keys and certificates. For most major servers this occurred within 48 hours. For many small businesses and organizations it may take months or longer before the process of patching OpenSSL and replacing certificates is implemented.

OpenSSL is an open-source implementation of Transport Layer Security (TLS), which developed out of the earlier Secure Sockets Layer (SSL) encryption. TLS forms the architecture for encrypted web-based communications.

When a user navigates a browser to a secure web site such as the login page for a bank account, the communications are encrypted using TLS. This is indicated by the URL address in the browser that prefaces encrypted connections with HTTPS rather than the standard HTTP (Hypertext Transfer Protocol).

OpenSSL is an open-source program. This means that the source code, the set of machine instructions, in this case written in the computer programming language C, are open for the public to read and contribute to. This means that it is possible to check that the code is secure and that the program is not secretly engaged in malicious or unwanted activity. Poorly maintained open-source programs can wind up a mess of contributions and suffer

unclear and inconsistent code.

OpenSSL has been regularly called “spaghetti code.” It is a jumble of opaque variables and convoluted subroutines that make it very hard to vet for security.

The OpenSSL source code, which serves as the security backbone of two-thirds of all Internet traffic, is maintained by four core programmers, only one of whom works on OpenSSL full-time. OpenSSL is funded by donations.

In February 2012, OpenSSL implemented what was known as a “heartbeat protocol.” The heartbeat protocol allowed the exchange of packets of information to insure that the client and the server to which it was connected were still actively communicating. In principle, the client would send a packet of data up to 64 kilobytes in size to the server, which would be stored in the server’s memory, and then transmitted back to the client, creating a steady “heartbeat” of data transmission.

In practice, however, because of an error in five lines of code in OpenSSL known as a “missing bounds check,” it was possible for a client to send a much smaller packet of data to the server and still request back 64k of data from memory. The server would send requested information to the client, randomly dumping whatever the contents of its memory were at the moment of the request. There was no limit to the number of times such an exfiltration of data could occur.

With fairly little effort, anyone familiar with the Heartbleed bug could obtain the private keys of the server and, with these, access every bit of data stored on it or transmitted to it.

It is possible that the five lines of code that produced what has been widely called the worst open security breach in the history of the Internet were the result of a programming mistake. Under the irrational and socially unplanned capitalist system, hundreds of billions of dollars are spent annually by firms in the pursuit of profit online, while the public security infrastructure for the digital communications of the majority of humanity is being developed by a handful of volunteers, whose average weekly donation income is measured in the hundreds of dollars.

It is entirely plausible, however, that the lines of bad OpenSSL code were planted by the National Security Agency (NSA). The revelations made by Edward Snowden of NSA spying revealed not only that the NSA is actively engaged in the surveillance and retention of every shred of digital communications, but that they also intentionally break its security architecture.

As part of its Bullrun program, the NSA crafted code with backdoors and vulnerabilities that were then incorporated into commercially available encryption software. Reuters revealed that the NSA secretly paid security company RSA $10 million to incorporate multiple layers of compromised cryptography into its widely used cryptographic library, BSAFE, which allows the NSA to access encrypted material by “backdoor” in seconds.

The same NSA crafted cryptography is used by Apple’s iOS and Microsoft Windows.

Whether Heartbleed originated as a mistake or was deliberately planted by the NSA, it is a near certainty that the NSA has been using it for the past two years. The NSA both employs large teams of programmers whose sole task is to scan the code of important security programs for vulnerabilities such as Heartbleed, and it also offers bounties for so-called “zero day exploits,” that is, it will pay any programmer who discovers a software vulnerability to quietly communicate their unpatched discovery to the NSA for exploitation.

Bruce Schneier, who along with Glenn Greenwald is one of five people with access to a complete set of the documents obtained by Edward Snowden, wrote of Heartbleed, “At this point, the probability is close to one that every target has had its private keys extracted by multiple intelligence agencies.” Schneier’s comments are in reference to the private keys that identify and encrypt server communications.

In response to the Heartbleed bug, the *New York Times* and other outlets have advised Internet users to replace all of their online passwords.