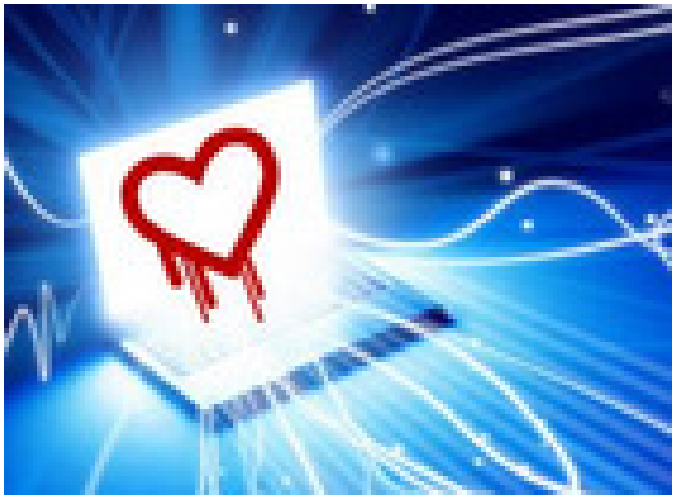
500,000+ Affected... Maybe Yours... Maybe Your Customers… What SPs Need to Know, Need to Do



Heartbleed, the newly discovered Internet flaw breaking the heart of the web industry and giving heart attacks to consumers, affects a half a million or more web sites. That's right, at least 500,000+ affected in this colossal open-source failure.

Why do we say "affected" and not "infected?"

Engineers working for the Finland-based security firm **Codenomicon** were exploring new features for their new security test software when they discovered the bug-heard-'round-the-world that affects websites that use OpenSSL, a security software that supposedly protected users' data and passwords.

A researcher from Google Security independently discovered the error at the same time.

You can recognize SSL protected sites because they have "https" (that "s" was for "secure") at the beginning of their Web addresses and usually display a "padlock icon" indicating the sites

are secure.

When Codenomicon was testing, something was wrong when they tried adding support for OpenSSL's "Heartbeat" extension, used to test whether a connection is secure like when exchanging data for passwords or credit card numbers.

Heartbeat allows one server to send arbitrary data to another. The recipient then sends back an exact replica of the data to the original sender to prove the security of the connection, to confirm nothing has been compromised.

But that's not what happened when Codenomicon tested. They noticed test cases that could trigger vulnerabilities within the Heartbeat protocol.

They found a flaw in the Heartbeat that could "bleed" extraneous data that any hacker using a simple script.

Heartbleed is particularly dangerous because OpenSSL is used across a majority of the Internet, so the bug likely affects almost every Internet user in one way or another.

Heartbleed is hard to detect because intruders can attack at an early phase of communication: essentially, a data thief can rob the building before the locks are put on the doors.

And that's why we say "affected" and not "infected." Nobody knows if data was leaked or not. The discovery of a flaw does not mean anyone has exploited it... (although rumors now allege the American spy agency NSA had knowledge and used this exploit).

In fact, there is a gap, a risky time between when the Good Guys announce a flaw to be corrected and the time it takes to be fixed. The Bad Guys learn the same way we do and can rush to exploit--when it was previously totally unknown to them.

The industry, by calling attention to the flaw, paints a target on every website-- and creates a Gold Rush for villains.

Ironically Codenomicon discovered that OpenSSL was even being used to power the company's own test protocol suite-- and it was leaking data.

Codenomicon patched its own servers and then brainstormed. A discovery like this makes a security company famous.

The company had internally named the bug "Heartbleed," so it purchased the domain name *hea rtbleed.com*
from a music lyrics site (still another site no doubt stricken by the SSL bug).

Codenomicon created a logo (to personify the bug), and began writing to the world about the problem, a problem that will also make their company famous, and some other firms jealous.

If Codenomicon caught the SSL flaw before thieves exploited it, the industry should be grateful. If they caught it after the exploit, the industry should still be thankful. In either case, they have rendered a true service. They are now heroes in the security industry. But being a hero is not easy…

For example, Reuters quotes a founder of the famous **Def Con** security conference who expressed frustration because his email and Web traffic vulnerability is nowposted on the Internet by others-- but he can't protect these assets until Intel releases a patch.

Def Con's network uses an enterprise firewall from McAfee (owned by Intel Corp's security division) that use affected versions of OpenSSL .

Was the bug a malicious flaw?

Nope, the guy who made the mistake has come forward and admitted his error created the bug.

OpenSSL is open source and has a listed volunteer crew of just 17 people. It turns out that in Dec. 2011, a bug was introduced in OpenSSL by volunteer German programmer Dr. Robin Seggelmann. He told
The Sydney Morning Herald
he wrote the code to help solve other problems, and it was reviewed by other members before being added to the OpenSSL software.



projects / openssl.git / commit

summary | shortlog | log | commit | commitdiff | tree
(parent: 84b6e27) | patch

PR: 2658

```
author     Dr. Stephen Henson <steve@openssl.org>
           Sat, 31 Dec 2011 23:59:57 +0100 (22:59 +0000)
committer  Dr. Stephen Henson <steve@openssl.org>
           Sat, 31 Dec 2011 23:59:57 +0100 (22:59 +0000)
commit     4817504d069b4c5082161b02a22116ad75f822b1
tree       7a85f6af852e34e5b80080b50d80741f6ab36c5a        tree | snapshot
parent     84b6e277d4f45487377d0159e82c356d750e1218        commit | diff

PR: 2658
Submitted by: Robin Seggelmann <seggelmann@fh-muenster.de>
Reviewed by: steve
```

No-one spotted the mistake until earlier this month.

Dr. Seggelmann said the flaw was missed by him and a reviewer, who appears to have been another volunteer, Dr. Stephen Henson, according to the logs.

Dr. Seggelmann says the mistake itself was 'trivial', but added that its effect is “clearly severe.”

Who is affected and how can you tell?

Some experts claim 66% of all internet sites have this vulnerability. Certainly some of the most important sites in the world had it-- at least up until a few days ago. Yahoo, Facebook, Google and the whole Who’s Who in web site attraction…

But it is not just web sites. We need to think also about printers, wireless access points, routers, switches—many of these devices and others use OpenSSL as a way for the device to communicate via a browser interface.

While larger web companies such as Twitter and Google have already said they've patched the the issue, other types of devices, from set-top boxes to traffic lights, may not ever get fixed because their systems are updated regularly.

Business owners can be held liable for any data breaches if they do not act reasonably to protect consumers, so that puts pressure on Solution Providers and integrators to make sure they and their customers take steps to fix sites.

Apple confirms all of its devices and web services are safe from the bug and that its devices never used the problematic software.

Google admits Android 4.1.1 is exposed but saysit is working with phone makers to patch devices using "Jelly Bean."

What if your business site or your customer’s is affected?

Don’t panic, but proceed methodologically. Contact all your customers and explain (if anything, that is the first step that might keep you out of a lawsuit if you are responsible for their sites.) Tell them about your own new security measures and recommend password changes AFTER the patches. There is little point in rushing to change before the sites have been patched and updated, otherwise your new passwords will also be exposed to the same issue.

Make a list of all your sites (and devices) and ask your customers to do same. The OpenSSL project has addressed the Heartbleed issue in its newest versions, so that can be a simple upgrade for business sites. Device makers need to be contacted about patches.

An online "Heartbleed test" has been created to determine if a site (or server) is vulnerable to the Heartbleed flaw.

Anyone running a vulnerable version of OpenSSL should upgrade immediately and then create new private keys. There’s no way to tell if you have been attacked so you should assume the worst. This should be at the top of every IT security teams’ to-do list.

Do not focus only on external-facing servers, or even on only your own servers. You should make a list of business partners, check with them or at least educate them on the seriousness of this bug in their IT infrastructure. Their vulnerability is your vulnerability: a chain is only as good as its weakest link.

Everyone should assume they are already compromised and act accordingly.

Security is in everybody’s best interest. Security solution providers should not hesitate to use their expertise **to offer a service to customers and potential customers…an audit to access vulnerability and a program to cure.**

It’s an IT industry mess that needs cleaning up, but the companies who do the cleaning will get paid and be heroes.

Go **What Can You Do**