HEARTBLEED IN A NUTSHELL

What is Heartbleed?

The **Heartbleed bug** (CVE_2014- 0160) is a serious vulnerability in the popular OpenSSL crypto library, used by about 2/3 of HTTPS servers (banks, e-commerce, etc.).

Heartbleed allows an attacker to read chunks of memory of the server, which may contain confidential data such as clients' names, passwords, and cookies.

Worse, attackers may **recover secret keys** of the server, potentially enabling impersonation of the service as well as eavesdropping on future or, sometimes, past sessions.

What makes it unique?

- **Long exposure:** The bug has left a large volume of private keys and other secrets exposed for 2 years.
- **Ease of exploitation:** No skills are required to exploit it.
- **Stealth:** Attacks leave no obvious trace.

Am I affected?

Everyone is 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.

What should I do?

OpenSSL 1.0.1g (release date: April 7, 2014) fixes the bug and has to be deployed as soon as possible.

One should assume that the secret keys of a vulnerable server ARE compromised. This implies that a **safe move** would be **to revoke compromised certificates, then reissue and redistribute new ones** (using fresh key pairs).

Can I detect the exploitation attempts?

Exploitation leaves no obvious trace in the logs.

Which OpenSSL versions are affected?

OpenSSL 1.0.1 through 1.0.1f (inclusive) are **vulnerable**
OpenSSL 1.0.1g is NOT vulnerable
OpenSSL 1.0.0 branch is NOT vulnerable
OpenSSL 0.9.8 branch is NOT vulnerable

The bug was introduced in December 2011 and has been out in the wild since OpenSSL release 1.0.1 in March 2012.

Is OpenSSL 1.0.1 widely used?

The vulnerable versions have been available for over two years and they have been adopted widely by current operating systems.

A major factor is that TLS 1.1 & 1.2 came available with the first vulnerable OpenSSL version (1.0.1) and security community has been pushing the TLS 1.2 due to the earlier attacks against TLS (such as the BEAST).

Has this been abused in the wild?

Most probably, although there is no public evidence.

Who found the Heartbleed bug?

The bug was independently discovered by a team of security engineers at Codenomicon security company and one security researcher from Google. Heartbleed was then responsibly disclosed to the OpenSSL team.

The name Heartbleed comes from the **Heartbeat** extension (in RFC6520), whose implementation contains the bug.

WHAT IS BEING LEAKED AND HOW TO RECOVER IT?

Leaked material classification	Leaked items and potential attack	How to recover
Primary key material	Encryption keys allow an attacker to decrypt any future traffic to the protected services and to impersonate the service at will. Past traffic may also be compromised, depending on the crypto protocols used.	Patching the vulnerability, revocation of the compromised keys, reissuing and redistributing new keys. Even these actions may still leave some traffic intercepted by the attacker in the past still vulnerable to decryption.
Second key material	User credentials (user names and passwords) used in the vulnerable services.	Restore trust to the primary key material. Change passwords and possible encryption keys that have been compromised. All session keys and session cookies should be invalided and considered compromised.
Protected content	Content handled by the vulnerable services: may be personal or financial details, private communication such as emails or instant messages, documents or anything seen worth protecting by encryption.	Restore trust to the primary and secondary key material as described above. Only this will ensure safe use of the compromised services in the future.
Collateral	Other details exposed to an attacker in the leaked memory content may be technical details, e.g.: memory addresses, security measures, such as canaries used to protect against overflow attacks.	Collateral material has only contemporary value and will lose it when OpenSSL has been upgraded to a fixed version.

KUDELSKI SECURITY