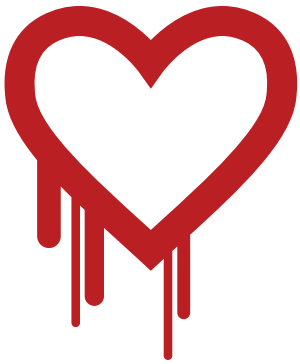

The Heartbleed Story

Heartbleed is a serious vulnerability that affects the Heartbeat extension of specific versions of OpenSSL. OpenSSL is an open source implementation of the Secure Socket Layer (SSL) protocol used to provide cryptographic services within a variety of control system hardware and software.

Bugs in software and software libraries come and go and are fixed by new versions, but Heartbleed is a very serious bug, because:

- It affects a very large share of Internet users (66% of all servers)
- It can be used to reveal very sensitive data
- It is easy to exploit
- Exploits don't leave a trace
- Long exposure time, 2 years

How was the bug discovered?

The vulnerability was discovered independently by researchers at Codenomicon and Google Security. Codenomicon researchers found the bug while improving the SafeGuard feature in Codenomicon's Defensics security testing tools. The researchers were able to attack the company's own servers from outside, without leaving a trace. Without using any privileged information or credentials, they were able steal the secret keys used in the company's X.509 certificates, employee user names and passwords, instant messages, emails and business critical documents and communication.

What is the impact of the bug?

Encryption keys are the crown jewels of network information. Leaked security keys allow the attacker to decrypt any past and future traffic to the protected services and to impersonate the service at will. In servers using vulnerable versions of OpenSSL, any protection given by the encryption and the signatures in the X.509 certificates can be bypassed.

What happened after discovery?

Immediately after discovering the bug, Codenomicon contacted the National Cyber Security Centre of Finland (NCSC-FI). The NCSC then took up the task of verifying the vulnerability, analyzing it further and reaching out to the authors of OpenSSL and software, operating system and appliance vendors, which were potentially affected.

Vulnerability coordination 2.0

Heartbleed is not Codenomicon's first big discovery. The company has been involved in hundreds of coordination processes, including several multi-vendor cases. However, this time, others went public with the bug much faster than expected. Based on their experiences in reporting vulnerabilities, they had a feeling that the Heartbleed called for "vulnerability coordination 2.0", i.e., making the information accessible to everyone as quickly as possible. Codenomicon published the Q&A list it had developed as a part of the coordination effort on the heartbleed.com website.

How to recover from Heartbleed?

Recovery from this leak requires patching the vulnerability, revocation of the compromised keys and reissuing and redistributing new keys. Codenomicon has launched a free tool for finding statically linked OpenSSL libraries from binaries, embedded devices and copy & pasted code. The tool available online at **appcheck.codenomicon.com**.

How to prepare for future attacks?

To avoid exposure to similar weaknesses in the future, organizations should constantly monitor applications and device firmware and use fuzzing to discover vulnerabilities. Attackers need to find a vulnerability in the code to devise attacks against a target system. If potential zero-day vulnerabilities are removed proactively, it becomes significantly harder for attackers to devise attacks.

SafeGuard

The SafeGuard feature in Codenomicon's Defensics security testing tools was original used to find the vulnerability. SafeGuard automatically tests the target system for weaknesses that compromise integrity, privacy or safety. It is a systematic solution for exposing failed cryptographic certificate checks, privacy leaks and authentication bypass weaknesses that expose Internet users to man in the middle attacks and eavesdropping.