

Heartbleed

“The attack is limited to data stored in computer memory”

Ilkka Sovanto



OpenSSL

- An open source crypto library, since 1998
- A very popular SSL/TLS implementation
- TLS promises secure transport between client and server
 - » Confidentiality
 - » Integrity

The vulnerability

- Vulnerable OpenSSL versions 1.0.1 – 1.0.1f.
- Created at end of 2011
- 1.0.1 released 14th March 2012
- TLS Heartbeat is like ping for TLS.
- Error in processing heartbeat messages

Discovery – the Finnish side

- Initial discovery on Thu April 3rd
- Riku from Codenomicon was testing new safety check features of their tools
- Later that afternoon NCSC-FI notified (EET)
- Ilkka and Jussi in Brussels

```
[02:34:11 PM] juhani.eronen%ficora.fi: mitäs löysitte?  
[02:34:30 PM] fenris: openssl vuotaa 65k muistia  
[02:34:33 PM] fenris: mahdollisesti avainmateriaalia  
[02:34:36 PM] fenris: preauth  
[02:34:41 PM] fenris: kumpaakin suuntaan  
[02:34:49 PM] fenris: ainakin certtejä yms. jo nähty  
[02:34:53 PM] fenris: siis vastauksiin  
[02:35:14 PM] juhani.eronen%ficora.fi: häh
```

Discovery – the Finnish side

- So, what did you find?
- Openssl leaks 65k chunks of memory
- Possibly keying material
- Preauth
- Both directions
- Saw certs etc. already
- Huh?

```
[02:34:11 PM] juhani.eronen%ficora.fi: mitäs löysitte?  
[02:34:30 PM] fenris: openssl vuotaa 65k muistia  
[02:34:33 PM] fenris: mahdollisesti avainmateriaalia  
[02:34:36 PM] fenris: preauth  
[02:34:41 PM] fenris: kumpaakin suuntaan  
[02:34:49 PM] fenris: ainakin certtejä yms. jo nähty  
[02:34:53 PM] fenris: siis vastauksiin  
[02:35:14 PM] juhani.eronen%ficora.fi: häh
```

Discovery – the Finnish side

- Offending code quickly located
 - » Impact limited to OpenSSL 1.0.1
 - » Plus any backports after Sat Dec 31 22:59:57 2011 +0000

Initial review

- Waiting for tool to reproduce from Codenomicon
- Where was the bad code used?
 - » Open source OS:es easy to check. Latest releases all had 1.0.1.
 - » Checked backports (1.0.x, 0.9.8) from several distros. Luckily nobody had backported heartbeat support.
 - » Products from most COTS vendors would use OpenSSL, so the vendor list would be extensive
 - » Most of the deployed SCADA products are likely too old

Partial list of affected products

- VMware ESXi 5.5
- VMware NSX-MH 4.x
- VMware NSX-V 6.0.x
- VMware NVP 3.x
- VMware vCenter Server 5.5
- VMware vFabric Web Server 5.0.x – 5.3.x
- VMware Fusion 6.0.x
- VMware Horizon Mirage Edge Gateway 4.4.x
- VMware Horizon View 5.3 Feature Pack 1
- VMware Horizon View Client for Android 2.1.x, 2.2.x,
- VMware Horizon View Client for iOS 2.1.x, 2.2.x,
- VMware Horizon View Client for Windows 2.3.x
- VMware Horizon Workspace 1.0
- VMware Horizon Workspace 1.5
- VMware Horizon Workspace 1.8
- VMware Horizon Workspace Client for Macintosh
- VMware Horizon Workspace Client for Macintosh
- VMware Horizon Workspace Client for Windows 1
- VMware Horizon Workspace Client for Windows 1
- VMware Horizon Workspace for Macintosh 1.8
- VMware Horizon Workspace for Windows 1.8
- VMware OVF Tool 3.5.0
- VMware vCloud Networking and Security (vCNS)
- VMware vCloud Networking and Security (vCNS)
- NetApp Clustered Data ONTAP® Antivirus Connector
- NetApp Data ONTAP® Storage Management Initiative Specification (SMI-5) Agent
- NetApp Manageability SDK (5.0P1 ja myöhemmät)
- NetApp OnCommand® Unified Manager Core Package (5.0 ja 5.1)
- NetApp OnCommand® Workflow Automation (2.2RC1)
- NetApp SnapProtect® (10.0 and service packs)
- NetApp Storage Management Initiative Specification (SMI-5) for E-Series
- Blue Coat Content Analysis System CAS 1.1.1.1 - 1.1.5.1
- Blue Coat Malware Analysis Appliance 1.1
- Blue Coat ProxyAV 3.5.1.1 - 3.5.1.6
- Blue Coat ProxySG 6.5.1.1 - 6.5.3.5
- Blue Coat SSL Visibility 3.7.0
- neXus Hybrid Access Gateway 5.2
- Barracuda Web Filter Version 7.0 - 7.1
- Barracuda Message Archiver Version 3.5 ja 3.6
- Barracuda Web Application Firewall Version 7.8
- Barracuda Link Balancer Version 2.5
- Barracuda Load Balancer Version 4.3 ja 4.4
- Barracuda Load Balancer ADC
- Barracuda Cudatel Version 3.0
- Barracuda Firewall 6.1
- Barracuda Cloud Control
- Barracuda Backup Service
- Barracuda Email Security Service
- Barracuda Copy
- Barracuda SignNow
- NGINX
- pfSense
- Oracle Communications Operations Monitor
- Oracle MySQL Enterprise Monitor
- Oracle MySQL Enterprise Server version 5.6
- Oracle Communications Session Monitor
- Oracle Linux
- Oracle Mobile Security Suite
- Oracle Solaris 11.2
- Oracle BlueKai
- Oracle Java ME - JSRs and Optional Packages
- Oracle Java ME - Mobile and Wireless
- Oracle MySQL Connector/C
- Oracle MySQL Connector/ODBC
- Oracle MySQL Workbench
- Oracle Communications Internet Name and Address Management
- Oracle Communications Application Session Controller
- Oracle Communications Interactive Session Recorder 5.1
- Oracle Communications Network Charging and Control
- Oracle Communications Session Delivery Management Suite
- Oracle Communications Session Monitor
- Oracle Communications WebRTC Session Controller
- Oracle Primavera P6 Prof Project Management
- McAfee Web Gateway
- McAfee Security for Linux
- McAfee Security for Mac OS X
- McAfee Security for Linux
- Dell SonicWALL SRA SMB Secure Remote Access (Server Side Firmware) 7.0.0.10-26sv ja vanhemmat 7.0 versiot, 7.5.0.3-19sv ja vanhemmat 7.5 versiot
- Dell SonicWALL SRA E-Class Secure Remote Access (Aventail) (E-Class SRA Server Software) Software version 10.6.4 versiot 10.7.0 ja 10.7.1
- Dell SonicWALL SRA Global Management System (GMS) and Analyzer GMS and Analyzer 7.2 (Windows versio)
- Extreme Networks Black Diamond Series X8, 8900 and 8800 EXOS versio 15.4.1
- Extreme Networks Summit Series X770 X670 X480 X460 X440

Partial list of affected products

- Debian Wheezy (korjattu versiossa openssl 1.0.1e-2+deb7u5)
- Ubuntu 12.04 LTS, 13.04 ja 13.10
- Gentoo Linux
- Slackware 14.0, 14.1 ja current
- OpenBSD 5.3 ja 5.4
- FreeBSD, versiot 10.x
- NetBSD, versiot 6.1 - 6.1.3 ja 6.0 - 6.0.4
- DragonflyBSD 3.6
- Mandriva Business Server 1
- CentOS 6.5
- Scientific Linux 6.5
- Oracle Linux
- F-Secure F-Secure Messaging Secure Gateway 7.5
- F-Secure Protection Service for Email 7.5
- F-Secure Anti-Theft Portal
- Synology versiota DSM 5.0-4458 Update 2 vanhemmat versiot
- Red Hat Enterprise Virtualization Hypervisor 6.5
- Red Hat Storage 2.1
- OpenVPN Access Server 1.8.4 - 2.0.5
- FortiGate (FortiOS) 5.0.0 - 5.0.6
- FortiClient 5.x
- FortiAuthenticator 3.x
- FortiMail 4.3.x and 5.x
- FortiVoice 200D, 200D-T ja VM
- FortiRecorder
- FortiADC D-Series 1500D, 2000D ja 4000D
- FortiADC E-Series 3.x
- Coyote Point Equalizer GX / LX 10.x
- FortiDDoS 4.x
- FortiDNS
- AscenLink v6.5 ja 7.0
- Cisco AnyConnect Secure Mobility Client for IOS
- Cisco Desktop Collaboration Experience DX650
- Cisco Unified 7800 series IP Phones
- Cisco Unified 8961 IP Phone
- Cisco Unified 9951 IP Phone
- Cisco Unified 9971 IP Phone
- Cisco TelePresence Video Communication Server (VCS)
- Cisco IOS XE Cisco UCS B-Series (Blade) Servers
- Cisco UCS C-Series (Stand alone Rack) Servers
- Cisco Unified Communication Manager (UCM) 10.0
- FortiGate FortiOS 5.0.5 ja 5.0.6
- Junos OS 13.3R1
- Juniper Odyssey client 5.6r5 ja sitä uudemmat versiot
- Juniper SSL VPN (IVEOS) 7.4r1 ja sitä uudemmat versiot
- Juniper SSL VPN (IVEOS) 8.0r1 ja sitä uudemmat versiot
- Juniper UAC 4.4r1 ja sitä uudemmat versiot
- Juniper UAC 5.0r1 ja sitä uudemmat versiot
- Juniper Junos Pulse (Desktop) 5.0r1 ja sitä uudemmat versiot
- Juniper Junos Pulse (Desktop) 4.0r5 ja sitä uudemmat versiot
- Juniper Network Connect (windows) versiot 7.4R5 - 7.8.0R3.1
- Juniper Junos Pulse (Mobile) on Android 4.2R1 ja sitä uudemmat versiot
- Juniper Junos Pulse (Mobile) on iOS 4.2R1
- F5 BIG-IP LTM versiot 11.5.0 - 11.5.1
- F5 BIG-IP AAM versiot 11.5.0 - 11.5.1
- F5 BIG-IP AFM versiot 11.5.0 - 11.5.1
- F5 BIG-IP Analytics versiot 11.5.0 - 11.5.1
- F5 BIG-IP APM versiot 11.5.0 - 11.5.1
- F5 BIG-IP ASM versiot 11.5.0 - 11.5.1
- F5 BIG-IP GTM versiot 11.5.0 - 11.5.1
- F5 BIG-IP Link Controller 11.5.0 - 11.5.1
- F5 BIG-IP PEM versiot 11.5.0 - 11.5.1
- F5 BIG-IP PSM versiot 11.5.0 - 11.5.1
- F5 BIG-IP Edge Clients for Apple iOS versiot 2.0.0 - 2.0.1 ja 1.0.5
- F5 BIG-IP Edge Clients for Linux versiot 7080 - 7101
- F5 BIG-IP Edge Clients for MAC OS X versiot 7080 - 7101 ja 6035 - 7071
- F5 BIG-IP Edge Clients for Windows versiot 7080 - 7101 ja 6035 - 7071
- OpenVPN 2.3-rc2-I001 - 2.3.2-I003
- Aruba ArubaOS versiot 6.3.x, 6.4.x
- Aruba ClearPass versiot 6.1.x, 6.2.x, 6.3.x
- Viscosity versiota 1.4.8 vanhemmat versiot
- WatchGuard XTM ja XCS, versiota 11.8.3 CSP vanhemmat versiot
- Blue Coat Content Analysis System versiot 1.1.1.1 - 1.1.5.1
- Blue Coat Malware Analysis Appliance versio 1.1.1
- Blue Coat ProxyAV versiot 3.5.1.1 - 3.5.1.6
- Blue Coat ProxySG versiot 6.5.1.1 - 6.5.3.5
- Blue Coat SSL Visibility 3.7.0
- Jolla

Partial list of affected products

- Debian Wheezy (korjattu versiossa openssl 1.0.1e-2+deb7u5)
- Ubuntu 12.04 LTS, 13.04 ja 13.10
- Gentoo Linux
- Slackware 14.0, 14.1 ja current
- OpenBSD 5.3 ja 5.4
- FreeBSD, versiot 10.x
- NetBSD, versiot 6.1 - 6.1.3 ja 6.0 - 6.0.4
- DragonflyBSD 3.6
- Mandriva Business Server 1
- CentOS 6.5
- Scientific Linux 6.5
- Oracle Linux
- F-Secure F-Secure Messaging Secure Gateway 7.5
- F-Secure Protection Service for Email 7.5
- F-Secure Anti-Theft Portal
- Synology versiota DSM 5.0-4458 Update 2 vanhemmat versiot
- Red Hat Enterprise Virtualization Hypervisor 6.5
- Red Hat Storage 2.1
- OpenVPN Access Server 1.8.4 - 2.0.5
- FortiGate (FortiOS) 5.0.0 - 5.0.6
- FortiClient 5.x
- FortiAuthenticator 3.x
- FortiMail 4.3.x and 5.x
- FortiVoice 200D, 200D-T ja VM
- FortiRecorder
- FortiADC D-Series 1500D, 2000D ja 4000D
- FortiADC E-Series 3.x
- Coyote Point Equalizer GX / LX 10.x
- FortiDDoS 4.x
- FortiDNS
- AscenLink v6.5 ja 7.0
- Cisco AnyConnect Secure Mobility Client for IOS
- Cisco Desktop Collaboration Experience DX650
- Cisco Unified 7800 series IP Phones
- Cisco Unified 8961 IP Phone
- Cisco Unified 9951 IP Phone
- Cisco Unified 9971 IP Phone
- Cisco TelePresence Video Communication Server (VCS)
- Cisco IOS XE Cisco UCS B-Series (Blade) Servers
- Cisco UCS C-Series (Stand alone Rack) Servers
- Cisco Unified Communication Manager (UCM) 10.0
- FortiGate FortiOS 5.0.5 ja 5.0.6
- Junos OS 13.3R1
- Juniper Odyssey client 5.6r5 ja sitä uudemmat versiot
- Juniper SSL VPN (IVEOS) 7.4r1 ja sitä uudemmat versiot
- F5 BIG-IP LTM versiot 11.5.0 - 11.5.1
- F5 BIG-IP AAM versiot 11.5.0 - 11.5.1
- F5 BIG-IP AFM versiot 11.5.0 - 11.5.1
- F5 BIG-IP Analytics versiot 11.5.0 - 11.5.1
- F5 BIG-IP APM versiot 11.5.0 - 11.5.1
- F5 BIG-IP ASM versiot 11.5.0 - 11.5.1
- F5 BIG-IP GTM versiot 11.5.0 - 11.5.1
- F5 BIG-IP Link Controller 11.5.0 - 11.5.1
- F5 BIG-IP PEM versiot 11.5.0 - 11.5.1
- F5 BIG-IP PSM versiot 11.5.0 - 11.5.1
- F5 BIG-IP Edge Clients for Apple iOS versiot 2.0.0 - 2.0.1 ja 1.0.5
- F5 BIG-IP Edge Clients for Linux versiot 7080 - 7101
- F5 BIG-IP Edge Clients for MAC OS X versiot 7080 - 7101 ja 6035 - 7071
- Juniper SSL VPN (IVEOS) 7.4r1 ja sitä uudemmat versiot 7080 - 7101 ja 6035 - 7071
- Juniper Junos Pulse (Mobile) on Android 4.2R1 ja sitä uudemmat versiot
- Juniper Junos Pulse (Mobile) on iOS 4.2R1
- Blue Coat Content Analysis System versiot 1.1.1.1 - 1.1.5.1
- Blue Coat Malware Analysis Appliance versio 1.1.1
- Blue Coat ProxyAV versiot 3.5.1.1 - 3.5.1.6
- Blue Coat ProxySG versiot 6.5.1.1 - 6.5.3.5
- Blue Coat SSL Visibility 3.7.0
- Jolla

Juniper SSL VPN (IVEOS) 7.4r1
 Juniper SSL VPN (IVEOS) 8.0r1

SSL VPN + no 2-factor auth?

Tue August 19, 2014

CHS Hacked via Heartbleed Vulnerability

As many of you may have already been aware, a breach at Community Health Systems (CHS) affecting an estimated 4.5 million patients was recently revealed. TrustedSec obtained the first details on how the breach occurred and new information relating to this breach. The initial attack vector was through the infamous OpenSSL “heartbleed” vulnerability which led to the compromise of the information.

This confirmation of the initial attack vector was obtained from a trusted and anonymous source close to the CHS investigation. Attackers were able to glean user credentials from memory on a CHS Juniper device via the heartbleed vulnerability (which was vulnerable at the time) and use them to login via a VPN.



Reproducing

- 20.35: Received the repro tool
- ~22.15: Successful repro (#!½x" Wireshark SSL decryption)
- A closer look at OpenSSL memory layout, Jussi working on improving the repro
- 23.42: Basic auth credentials leaked. A lot of other traffic data before that
- Studying private key representation in memory
- 02:45 April 4th: RSA private exponent leaked

Implications

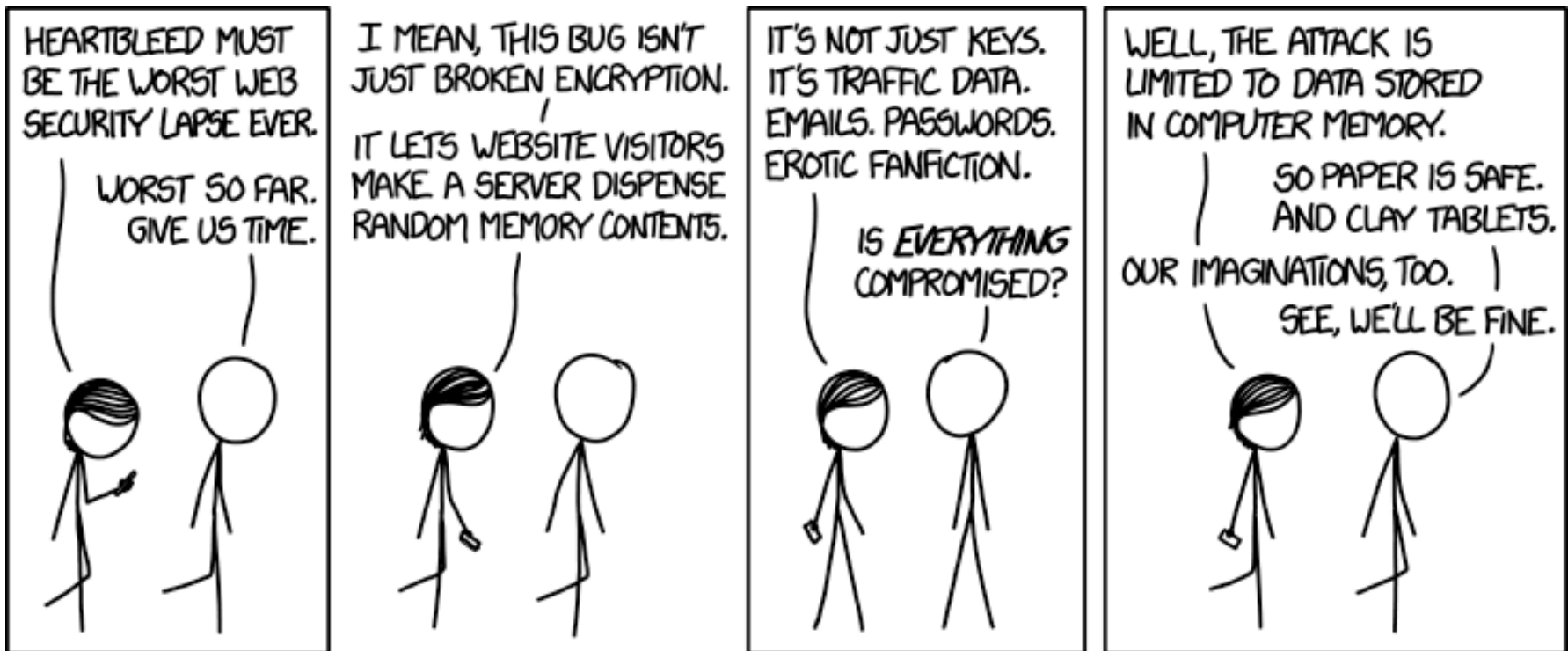
[11:48:02 PM] juhani.eronen%ficora.fi: nsa:lla tulee paljon facepalma jos eivät oo tajunneet laittaa heartbeattia joka paikkaan ;)

[11:48:10 PM] fenris: :D

[11:48:11 PM] fenris: :D

[11:48:21 PM] fenris: saattaapi vituttaa juu

[11:48:45 PM] fenris: kiitos, tuo piristi :)



© xkcd.com

Implications

- Exploitation leaves no traces on target system
- Encryption support!
- Personal information, user credentials
 - » Password reuse between systems
- Admin credentials
 - » Allow system compromise
- Private key leak
 - » Allows MiTM
 - » Allows decryption of past data -> PFS!
- Any other sensitive information

What now?

- So, certificates from vulnerable services need to be changed.
- Then passwords.
- Then perhaps session cookies and other data

Open questions

- Can the private key leak be reproduced in real systems?
- How widespread is OpenSSL 1.0.1 use?
- Which closed-source products use it? How to handle contacting all of them?
- Which critical systems use it?
- Are there mitigations? How hard is the patch to create?
- Is this vulnerability already known by someone?
- Can the certificate change actually be done at scale?

Impact assessment

- Codenomicon created a simpler s_client PoC to test for the vulnerability (send hb at a command and check for response length).
- We created a simple Python PoC based on the s_client version
- I tested various services and could leak private keys from them. We and Codenomicon tested our own systems and could leak data from them.
- Spot checks (yahoo, google, ...) suggested they're vulnerable (only checked returned data amount)
- Oh dear.

Mitigation

- The config flag `-DOPENSSL_NO_HEARTBEATS` seemed to work. Created packages for CentOS/Ubuntu and they were found not vulnerable. Patched our systems.
- Did not want to bang our heads against the wall so much as to create a real patch.

```
[11:50:45 PM] fenris: oikeasti tuota openssl:n koodia,
en taida enää katsoa sitä tälle iltaa
[11:50:55 PM] juhani.eronen%ficora.fi: :D
[11:51:00 PM] juhani.eronen%ficora.fi: tajuttiin taas
jottain muuten
[11:51:06 PM] fenris: siellä kopsaillaan noita avaimia
niin paljon ja osassa paikkaa on pkey:ssä vissiin
private ja osassa public key
[11:51:11 PM] juhani.eronen%ficora.fi: :D :D
[11:51:16 PM] fenris: pkey-nimisessä muuttujassa
[11:51:17 PM] fenris: siis
[11:51:21 PM] fenris: hienoa
[11:51:26 PM] juhani.eronen%ficora.fi: jee
```

Monitoring

- Codenomicon created a logging version of s_server to monitor for attacks. The first honeypots were running on April 4. On April 7, they were replaced with modified Apache servers.
- An existing honeynet was used to host the modified server.
- The honeynet consisted of 2000-3000 IP addresses, mostly in Finland.
- We made Snort rules to detect heartbleed attacks and employed them in HAVARO.

Coordination plan

- Craft good materials describing the vulnerability in detail (ended up with QA form). Craft technical materials describing the vulnerability and its impact (there was some text already).
- Make a preliminary vendor list
- Get a CVE number
- Contact the OpenSSL team, suggest a way forward
- Contact vultures to distribute the vendor contact load
- A few days before the scheduled date, contact distros, trusted certs and CNI providers
- Coordinated publication

Branding

- Codenomicon had the idea to brand the bug, give it a better name than CVE-X and to create a plain language description of the vulnerability and its impact.
- As the vulnerability is quite serious, this was thought to answer the need of information from the general public and the media.



Heartbleed.com

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.



Coordination – first steps

- On April 7 we notified our bosses about the vulnerability, asked for more resources. First list of critical Finnish services drafted.
- Contacted vultures for pre-notification (“a critical issue in OpenSSL”) and received a CVE on April 6, received one on April 7 at 16.24 from CERT/CC.
- We and Codenomicon had handled numerous cases with OpenSSL before (previous contact related to another case on April 7 at 14.20).
- Sent OpenSSL a detailed report at 18.19, containing our ideas on the coordination flow.

Coordination – how it occurred

- OpenSSL had been contacted about the vulnerability earlier by Neel Mehta of Google.
- Prior to our contact, they had been suspecting someone leaking the vulnerability to 3rd parties.
- → OpenSSL deemed the risk of not publishing too high, and put the report out at around 21.00 on April 7.
- We were not notified in any way, Marko from Codenomicon phoned Jussi.

Co-discovery – really?

- Yep, it happens
- Recent events drive research interest towards similar goals
 - » Apple goto fail
 - » GnuTLS goto cleanup

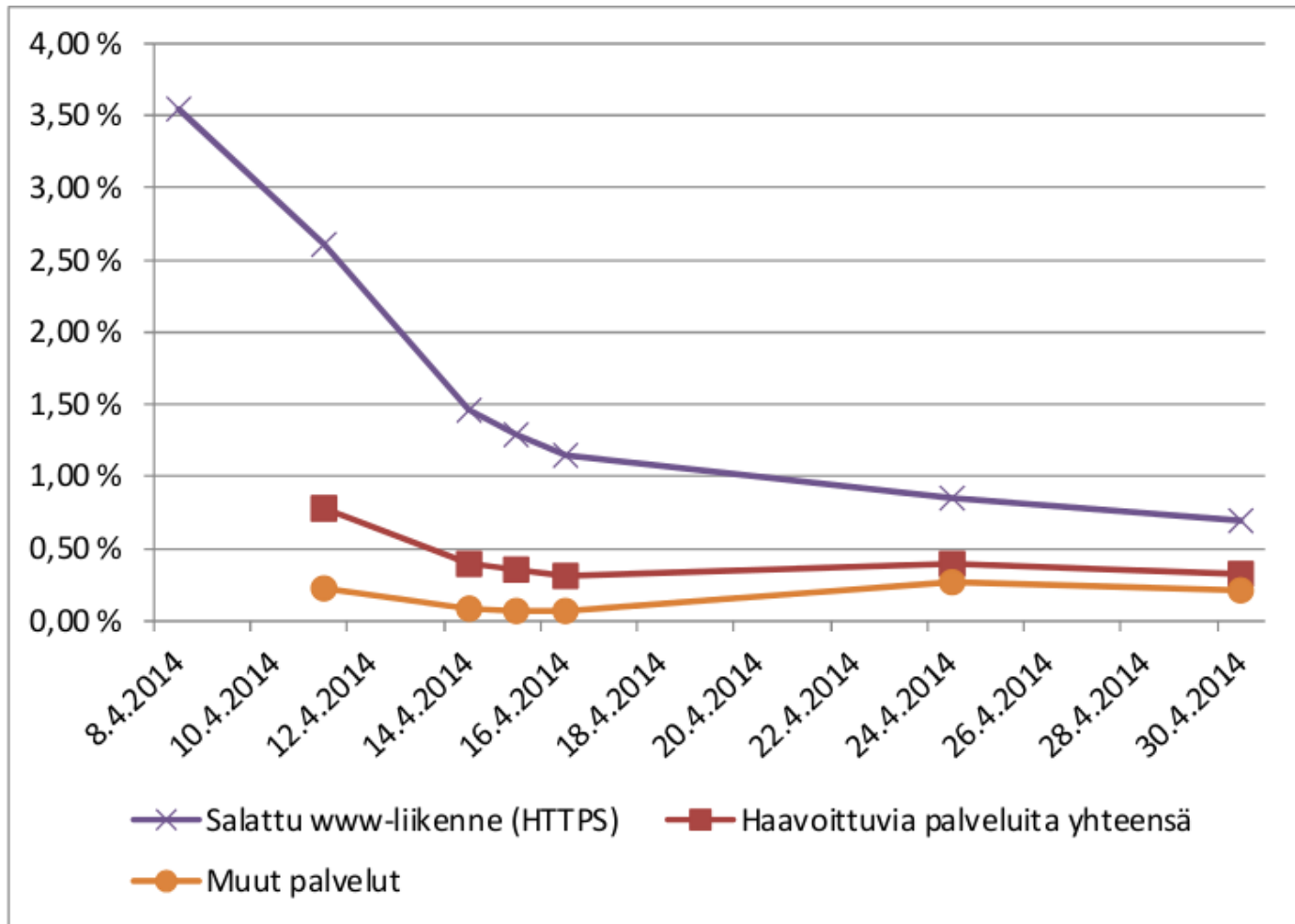
The aftermath

- We decided that the QA materials we had produced should be made public immediately. Codenomicon used heartbleed.com for this.
- First hits in the honeypots came around 23.00 on April 7. The slow development of sophistication and scope of scans was kind of fun to watch.
- We published our advisory and warning in the morning of April 8. There was a lot of briefing to be done. The vulnerability scanners were still in a bit rough state (developed by OUSPG).
- First systematic scans of critical Finnish systems.

The aftermath

- We scanned the entire Finnish IP space for vulnerabilities. Scans were constantly reported with our automatic tools.
- Improved the scanner, there were lot of bugs producing false negatives.
- Made a virtual machine scanner for the government.

The aftermath



The great private key controversy



Neel Mehta

@neelmehta

+ Follow

Heap allocation patterns make private key exposure unlikely for [#heartbleed](#) [#dontpanic](#).

↩ Reply ↻ Retweet ★ Favorite ⋮ More

RETWEETS

282

FAVORITES

86



1:08 PM - 8 Apr 2014

The great private key controversy

Conclusions

We think the stealing private keys on most NGINX servers is at least extremely hard and, likely, impossible. Even with Apache, which we think may be slightly more vulnerable, and we do not use at CloudFlare, we believe the likelihood of private SSL keys being revealed with the Heartbleed vulnerability is very low. That's about the only good news of the last week.

Wednesday, April 09, 2014

Why heartbleed doesn't leak the private key [retracted]

By [Robert Graham](#)

I got this completely wrong!

So as it turns out, I completely messed up reading the code. I don't see how, but I read it one way. I can still visualize the code in my mind's eye that I thought I read -- but it's not the real code. I thought it worked one way, but it works another way.


Private keys are still not so likely to be exposed, but still much more likely than my original analysis suggested.

The incorrect post is below, so you know how wrong I was

The CloudFlare challenge

CFP Heartbleed Challenge

← → ↻ <https://www.cloudflarechallenge.com/heartbleed>

 CLOUDFLARE

The Heartbleed Challenge

Can you steal the keys from this server?

Has the challenge been solved yet? **NO.**

This server is running nginx-1.5.13 linked against OpenSSL 1.0.1.f on Ubuntu 13.10 x86_64. It is vulnerable to [Heartbleed](#). Can you get the secret key?

If you think you have it, submit the RSA signature of the string " as proof. This proof can be obtained via the Heartbleed bug.

This site is vulnerable!
The domain www.cloudflarechallenge.com could be vulnerable to the Heartbleed SSL bug.

RETWEETS

399

FAVORITES

128



6:41 AM - 11 Apr 2014

Why I solved the challenge

- A great way to demonstrate the problem without helping the script kiddies
- My tools were ready
- Left tools running on Friday night while preparing food
- Checked every now and then if I caught anything
 - » Public modulus % candidate number = 0?

```
$ python keyhunt.py tocheck1/*.dump  
found prime c4ea13ad234ee22bf93337f332a74935fd1c0f195d3840...  
other prime c9d599dfcb3ace7a66070d410c173c6f70d15c60610d66...  
d: (assumed e = 65537) 2994cbb69875407323991527d1b3195a9...  
filename: tocheck1/1397254086-0-16726.dump
```


The future

- Many efforts to improve the security of OpenSSL
 - » New funding, full time employees
 - » LibreSSL, BoringSSL, ...
- The long tail is long
 - » Many embedded devices might never get patches

Shellshock – a quick comparison

- Bash running code from env variables
- Need a service that passes user input via env
 - » And calls bash at some point
- Examples
 - » Webservers with CGI applications
 - cPanel
 - Need to know the path to a suitable CGI script
 - » Services that allow user-configured hooks
 - DHCP client
 - OpenVPN
 - Some SIP servers

Shellshock – a quick comparison

Heartbleed

- Leaks sensitive information
- Straightforward attack vector
- Most vulnerable targets are exploitable
- Can be scanned or attacked relatively safely, straightforward
- Stealthy

Shellshock

- Gives full or partial control
- Multiple attack vectors
- Exploitation requires a service that passes user input through environment to bash
- No single way to attack
- Quite visible
 - » ... maybe



**Finnish Communications
Regulatory Authority**
National Cyber Security Centre

www.ncsc.fi
www.ficora.fi
