Odkrivanje ranljivih strežnikov na heartbleed napad v slovenskem naslovnem prostoru

arnes

Anton Brne
si·cert

Heartbeat

SI-CERT 2014-03 / OpenSSL kritična ranljivost

sreda, 09.04.2014

Opis

Programska knjižnica OpenSSL vsebuje resno varnostno pomanjkljivost pri implementaciji razširitve heartbeat protokola TLS in DTLS. S posebej prirejenim zahtevkom lahko napadalec prebere 64kB podatkov iz delov pomnilniškega prostora strežnika, kjer se lahko nahajajo zelo občutljivi podatki, kot so avtentikacijski podatki o uporabnikih – gesla, sejni piškotki, in tudi zasebni ključ strežnika. Napad ne pušča sledi v dnevniških datotekah, zato po trenutno znanih podatkih ne vemo, ali se je ranljivost izkoriščala v napadih že pred 7.4.2014, ko je bila ranljivost javno objavljena.

Ranljive verzije

OpenSSL verzije 1.0.1 do vključno 1.0.1f.

Verzije, ki **niso** ranljive:

- OpenSSL 1.0.1g,
- OpenSSL 1.0.0 (celotna veja),
- OpenSSL 0.9.8 (celotna veja).

Ranljivi so tako strežniki, kot tudi klienti, ki temeljijo na ranljivi verziji programske knjižnice OpenSSL.

si·cert

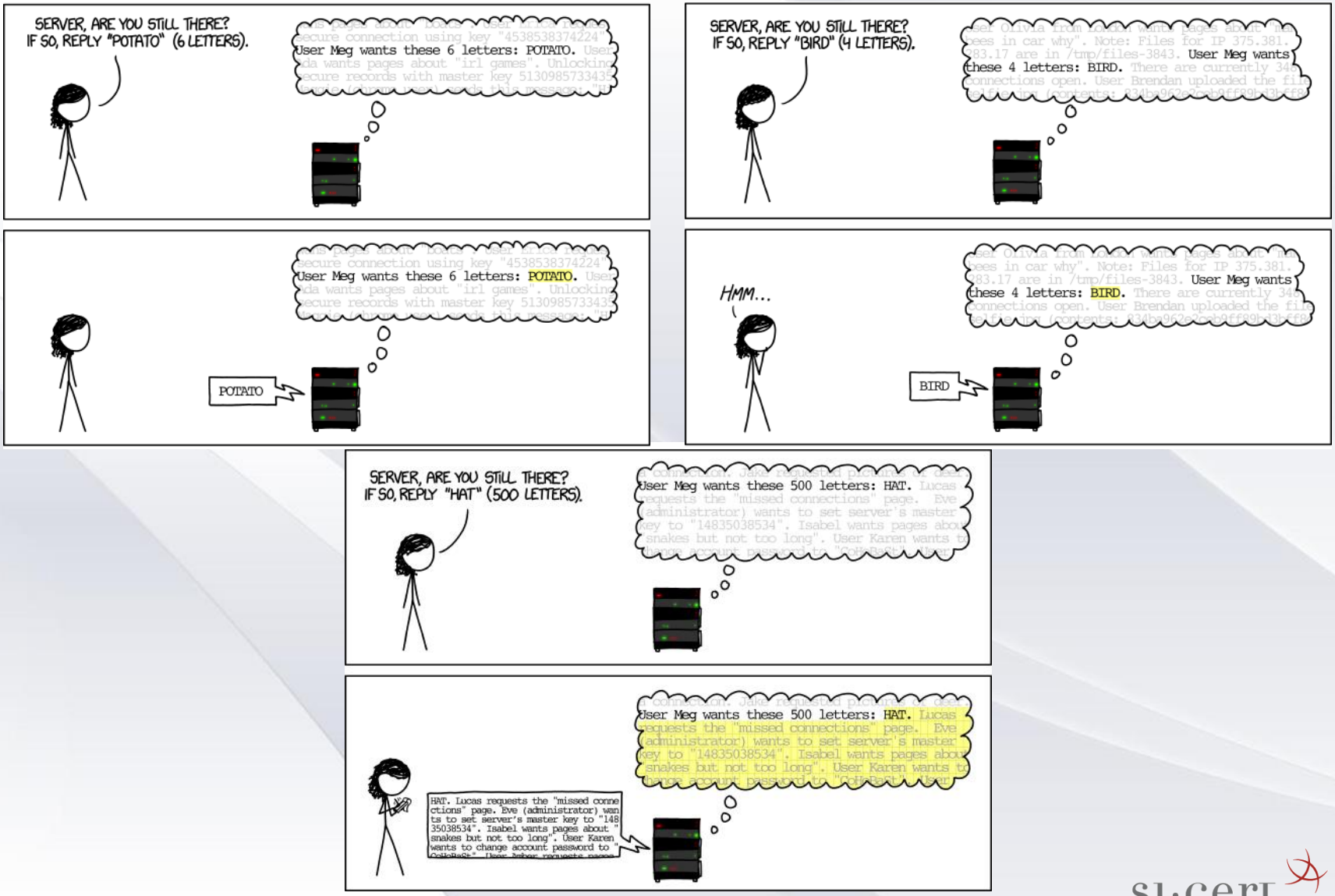
Heartbeat

Author	Dr. Stephen Henson <steve@openssl.org>
	Sun, 1 Jan 2012 00:59:57 +0200 (22:59 +0000)
Committer	Dr. Stephen Henson <steve@openssl.org>
	Sun, 1 Jan 2012 00:59:57 +0200 (22:59 +0000)
Commit	4817504d069b4c5082161b02a22116ad75f822b1
Tree	7a85f6af852e34e5b80080b50d80741f6ab36c5a
Parent	84b6e277d4f45487377d0159e82c356d750e1218

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

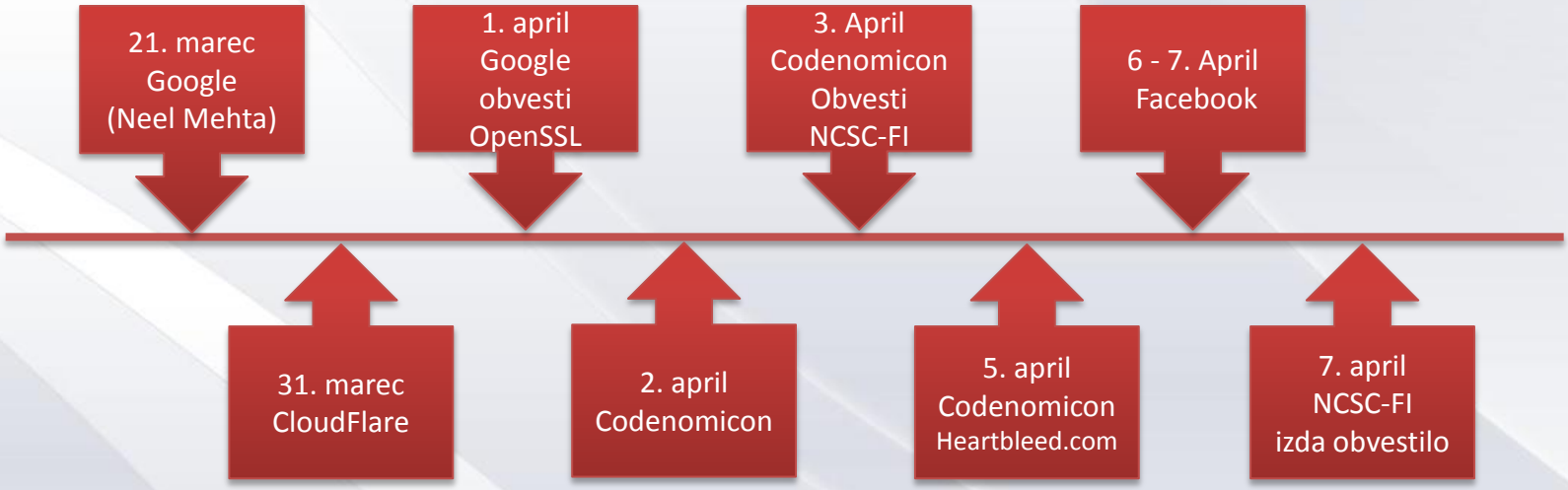
Support for TLS/DTLS heartbeats.

HOW THE HEARTBLEED BUG WORKS:



si·cert

Časovnica odkrivanja Heartbleed ranljivosti



Kdo je vedel?

Google , CloudFlare , OpenSSL, Codenomicon , National Cyber Security Centre Finland , Akamai in Facebook. Tik pred objavo pa tudi SuSE, Debian, FreeBSD in AltLinux.

Kdo ni vedel?

Amazon, Twitter, Yahoo, Ubuntu, Cisco, Juniper, Pinterest, Tumblr, GoDaddy, Flickr, Minecraft, Netflix, Instagram, Box, Dropbox, GitHub, Wikipedia, Wordpress, Wunderlist …

si·cert

SIX route collector

```
inet.0: 1493 destinations, 2593 routes (1491 active, 0 holddown, 2 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 110w5d 19:44:14
                    > to 88.200.2.194 via lt-0/0/0.7
5.8.32.0/21        *[BGP/170] 13:07:01, MED 0, localpref 100
                      AS path: 39912 39792 44050 I
                    > to 91.220.194.116 via ge-2/3/0.0
5.8.40.0/21        *[BGP/170] 13:07:01, MED 0, localpref 100
                      AS path: 39912 39792 44050 I
                    > to 91.220.194.116 via ge-2/3/0.0
5.8.64.0/21        *[BGP/170] 13:07:01, MED 0, localpref 100
                      AS path: 39912 39792 44050 I
                    > to 91.220.194.116 via ge-2/3/0.0
5.8.88.0/22        *[BGP/170] 13:07:01, MED 0, localpref 100
                      AS path: 39912 39792 44050 I
                    > to 91.220.194.116 via ge-2/3/0.0
5.8.92.0/22        *[BGP/170] 3w5d 18:45:53, MED 0, localpref 100
                      AS path: 39912 39792 44050 I
                    > to 91.220.194.116 via ge-2/3/0.0
5.23.104.0/21      *[BGP/170] 13:07:01, MED 0, localpref 100
                      AS path: 39912 39792 41854 57214 I
                    > to 91.220.194.116 via ge-2/3/0.0
5.32.136.0/21      *[BGP/170] 5d 04:05:39, localpref 1, from 91.220.194.1
                      AS path: 44549 I
                    > to 91.220.194.21 via ge-2/3/0.0
                    [BGP/170] 5d 04:14:47, localpref 1, from 91.220.194.101
```

si·cert

SIX route collector

48894	193.9.21.165	193.9.21.0/24	SI	ripencc	2009-02-24	ISG-AS ISG projektiranje in inzeniring, d.o.o.,SI
57127	146.247.24.167	146.247.24.0/24	SI	ripencc	2011-07-13	ISERVER-AS iSERVER informacijske storitve d.o.o.,SI
34779	188.230.215.187	188.230.192.0/19	SI	ripencc	2009-07-30	T-2-AS T-2, d.o.o.,SI
34779	188.230.175.167	188.230.160.0/19	SI	ripencc	2009-07-30	T-2-AS T-2, d.o.o.,SI
58046	84.39.214.104	84.39.208.0/20	SI	ripencc	2012-09-05	HKOM-AS Ministrstvo za notranje zadeve,SI
42560	5.43.64.184	5.43.64.0/18	BA	ripencc	2012-05-18	BA-TELEMACH-AS Telemach d.o.o. Sarajevo,BA
2107	193.2.158.15	193.2.0.0/16	SI	ripencc		ARNES-NET ARNES,SI
35370	87.243.156.26	87.243.128.0/18	AT	ripencc	2005-07-25	AINET-AS Ainet Telekommunikations-Netzwerk Betriebs GmbH,AT
2107	193.2.241.14	193.2.0.0/16	SI	ripencc		ARNES-NET ARNES,SI
50344	193.104.236.185	193.104.236.0/24	SI	ripencc	2009-12-22	SI-CDE CDE nove tehnologije d.o.o.,SI
41630	193.219.100.117	193.219.100.0/24	SI	ripencc	2006-09-26	HELIOS-AS Helios Domzale d.d.,SI
5603	193.77.226.122	193.77.192.0/18	SI	ripencc		SIOL-NET Telekom Slovenije d.d.,SI
48943	195.88.167.135	195.88.166.0/23	AT	ripencc	2009-03-31	KAPPERNET KAPPER NETWORK-COMMUNICATIONS GmbH,AT
5603	89.143.229.243	89.143.192.0/18	SI	ripencc	2006-03-03	SIOL-NET Telekom Slovenije d.d.,SI
34502	85.199.16.215	85.199.0.0/18	AT	ripencc	2005-02-01	XLINK-AS Multikom Austria Telekom GmbH,AT
5603	193.77.225.131	193.77.192.0/18	SI	ripencc		SIOL-NET Telekom Slovenije d.d.,SI
34779	93.103.142.83	93.103.128.0/19	SI	ripencc	2008-03-14	T-2-AS T-2, d.o.o.,SI
34779	93.103.46.124	93.103.32.0/19	SI	ripencc	2008-03-14	T-2-AS T-2, d.o.o.,SI
57127	146.247.24.84	146.247.24.0/24	SI	ripencc	2011-07-13	ISERVER-AS iSERVER informacijske storitve d.o.o.,SI
39912	78.142.122.236	78.142.64.0/18	AT	ripencc	2007-07-31	I3B-AS i3B - Internetbreitband GmbH,AT
5603	193.77.54.174	193.77.0.0/18	SI	ripencc		SIOL-NET Telekom Slovenije d.d.,SI
34779	188.230.234.241	188.230.224.0/19	SI	ripencc	2009-07-30	T-2-AS T-2, d.o.o.,SI
50195	164.8.96.26	164.8.0.0/16	SI	ripencc		UM University of Maribor,SI
34779	84.255.203.148	84.255.192.0/18	SI	ripencc	2004-12-14	T-2-AS T-2, d.o.o.,SI
39912	78.142.108.117	78.142.64.0/18	AT	ripencc	2007-07-31	I3B-AS i3B - Internetbreitband GmbH,AT
34779	84.255.209.96	84.255.192.0/18	SI	ripencc	2004-12-14	T-2-AS T-2, d.o.o.,SI
34779	89.212.161.68	89.212.128.0/18	SI	ripencc	2006-05-03	T-2-AS T-2, d.o.o.,SI
29276	213.229.192.49	213.229.192.0/18	SI	ripencc	2003-05-05	MOBITEL-GPRS Telekom Slovenije, d.d.,SI
8307	195.210.237.52	195.210.192.0/18	SI	ripencc		Telekom Slovenije d.d.,SI
35140	80.79.183.226	80.79.176.0/20	RU	ripencc	2005-03-22	SPIN CJSC Race Telecom,RU
2107	141.255.199.105	141.255.192.0/18	SI	ripencc	2011-07-06	ARNES-NET ARNES,SI
2107	141.255.227.129	141.255.192.0/18	SI	ripencc	2011-07-06	ARNES-NET ARNES,SI
41104	195.95.173.169	195.95.173.0/24	SI	ripencc	2006-06-02	PODRAVKA-AS Podravka d.o.o.,SI
42560	93.180.120.103	93.180.96.0/19	BA	ripencc	2011-12-01	BA-TELEMACH-AS Telemach d.o.o. Sarajevo,BA
5603	193.77.222.121	193.77.192.0/18	SI	ripencc		SIOL-NET Telekom Slovenije d.d.,SI
2107	193.2.13.103	193.2.0.0/16	SI	ripencc		ARNES-NET ARNES,SI
42484	77.73.24.238	77.73.24.0/21	RU	ripencc	2007-03-01	GPTEL-AS Grand Prix Telecom AS,RU
35140	217.21.103.62	217.21.96.0/20	RU	ripencc	2004-08-02	SPIN CJSC Race Telecom,RU
5603	193.77.143.182	193.77.128.0/18	SI	ripencc		SIOL-NET Telekom Slovenije d.d.,SI
5603	89.143.109.152	89.143.64.0/18	SI	ripencc	2006-03-03	SIOL-NET Telekom Slovenije d.d.,SI
39792	81.91.181.69	81.91.176.0/20	RU	ripencc	2006-04-26	ANDERS-AS Anders Telecom Ltd.,RU
57127	146.247.24.206	146.247.24.0/24	SI	ripencc	2011-07-13	ISERVER-AS iSERVER informacijske storitve d.o.o.,SI
8591	90.157.161.194	90.157.128.0/17	SI	ripencc	2006-11-17	AMIS AMiS,SI

si·cert

Metoda pregleda

uporabljena orodja

https://zmap.io/

```
# zmap -p 443 -f "saddr,daddr,sport" -o sloIPv4.csv SIX_naslovni_prostor.txt
```

```
May 05 12:20:01.955 [INFO] zmap: output module: csv
0:01 1%; send: 30996 30.7 Kp/s (30.0 Kp/s avg); recv: 422 421 p/s (408 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.36%
0:02 2%; send: 59679 28.7 Kp/s (29.3 Kp/s avg); recv: 858 435 p/s (421 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.44%
0:03 2%; send: 86204 26.5 Kp/s (28.4 Kp/s avg); recv: 1234 375 p/s (406 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.43%
0:04 3%; send: 116439 30.2 Kp/s (28.9 Kp/s avg); recv: 1674 439 p/s (414 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.44%
0:05 4% (1m40s left); send: 854649 27.9 Kp/s (27.5 Kp/s avg); recv: 12919 428 p/s (416 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.51%
0:06 5% (1m39s left); send: 881576 26.9 Kp/s (27.5 Kp/s avg); recv: 13356 436 p/s (416 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.52%
…
1:39 99% (1s left); send: 3400960 done (26.9 Kp/s avg); recv: 52010 0 p/s (390 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.53%
1:40 100% (0s left); send: 3400960 done (26.9 Kp/s avg); recv: 52010 0 p/s (387 p/s avg); drops: 0 p/s (0 p/s avg); hits: 1.53%
May 05 12:21:41.050 [INFO] zmap: completed
```

```
# less sloIPv4.csv
saddr, daddr, sport
193.2.12.230,212.235.232.234,443
193.2.241.80,212.235.232.234,443
193.2.241.58,212.235.232.234,443
193.2.70.224,212.235.232.234,443
193.2.44.54,212.235.232.234,443
193.2.9.200,212.235.232.234,443
```

00:01:40:00

si·cert

Metoda pregleda

uporabljena orodja

http://nmap.org/

```
# nmap -Pn -p 443 --script=ssl-heartbleed.nse -iL sloIPv4.csv -oN ranljivi_heartbleed_SIX_IP.txt
```

01:31:00:00

```
# Nmap 6.00 scan initiated Mon May 5 12:23:07 2014
  as: nmap -Pn -p 443 --script=ssl-heartbleed.nse -iL sloIPv4.csv -oN ranljivi_heartbleed_SIX_IP.txt

Nmap scan report for 193.2.252.20
Host is up (0.0027s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing
information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|     Description:
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed
bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of
otherwise encrypted confidential information as well as the encryption keys themselves.
|
|     References:
|       http://www.openssl.org/news/secadv_20140407.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://cvedetails.com/cve/2014-0160/
```

si·cert

Metoda pregleda

uporabljena orodja

http://www.perl.org/

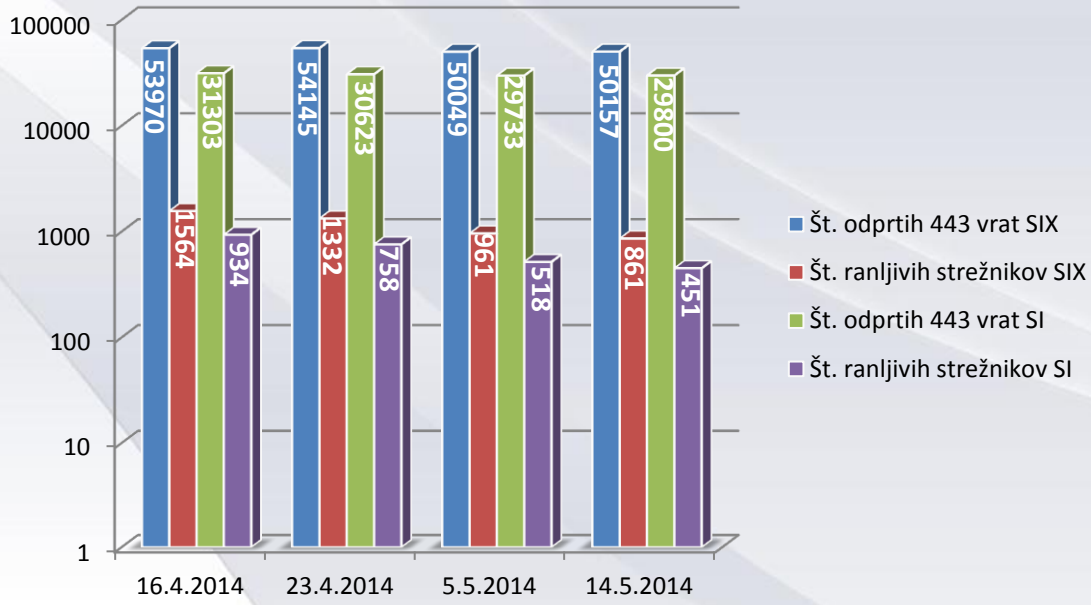
```
# perl check-ssl-heartbleed.pl -s 193.2.252.20
```

```
...ssl received type=22 ver=0x301 ht=0x2 size=54
...ssl received type=22 ver=0x301 ht=0xb size=755
...ssl received type=22 ver=0x301 ht=0xc size=393
...ssl received type=22 ver=0x301 ht=0xe size=0
...send heartbeat_
...ssl received type=24 ver=301 size=16384
BAD! got 16384 bytes back instead of 3 (vulnerable)
02 40 00 d8 03 01 53 43 5b 90 9d 9b 72 0b bc 0c  .@....SC[...r...
bc 2b 92 a8 48 97 cf bd 39 04 cc 16 0a 85 03 90  .+..H...9.......
9f 77 04 33 d4 de 00 00 66 c0 14 c0 0a c0 22 c0  .w.3....f.....".
21 00 39 00 38 00 88 00 87 c0 0f c0 05 00 35 00  !.9.8.........5.
84 c0 12 c0 08 c0 1c c0 1b 00 16 00 13 c0 0d c0  ................
03 00 0a c0 13 c0 09 c0 1f c0 1e 00 33 00 32 00  ............3.2.
9a 00 99 00 45 00 44 c0 0e c0 04 00 2f 00 96 00  ....E.D...../...
41 c0 11 c0 07 c0 0c c0 02 00 05 00 04 00 15 00  A...............
12 00 09 00 14 00 11 00 08 00 06 00 03 00 ff 01  ................
00 00 49 00 0b 00 04 03 00 01 02 00 0a 00 34 00  ..I...........4.
32 00 0e 00 0d 00 19 00 0b 00 0c 00 18 00 09 00  2...............
0a 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
04 00 05 00 12 00 13 00 01 00 02 00 03 00 0f 00  ................
10 00 11 00 23 00 00 00 0f 00 01 01 00 00 00 00  ....#...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
... repeated 1009 times ...
```

sl·cert

Rezultati pregleda

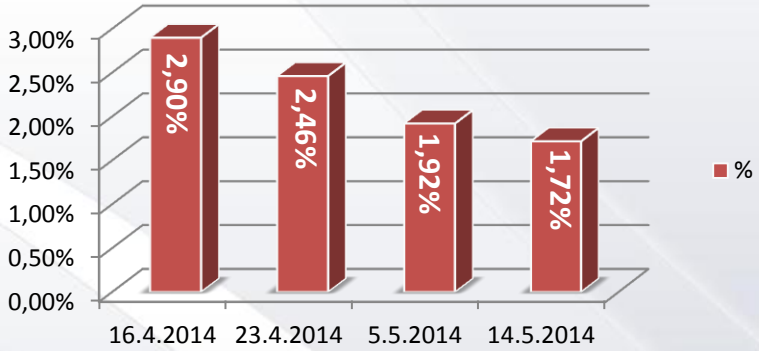
Datum	Št. odprtih 443 vrat SIX	Št. ranljivih strežnikov SIX	%	Št. odprtih 443 vrat SI	Št. ranljivih strežnikov SI	%
16.4.2014	53970	1564	2,90%	31303	934	2,98%
23.4.2014	54145	1332	2,46%	30623	758	2,48%
5.5.2014	50049	961	1,92%	29733	518	1,74%
14.5.2014	50157	861	1,72%	29800	451	1,51%



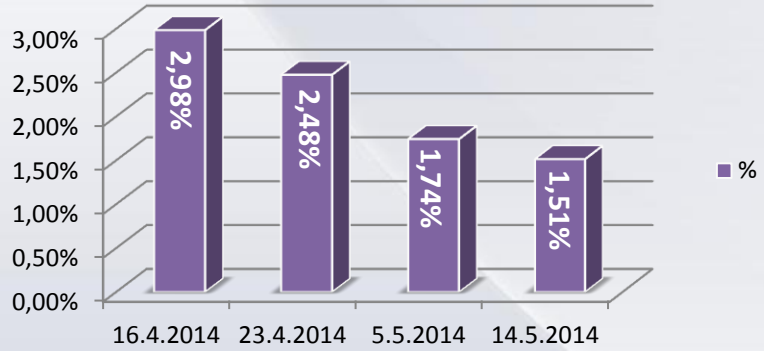
si·cert

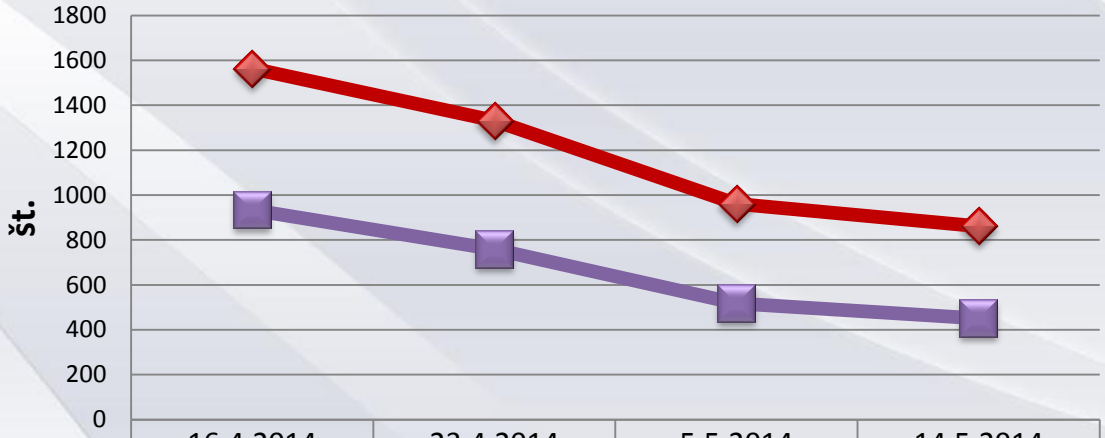
Rezultati pregleda

% ranljivih strežnikov SIX



% ranljivih strežnikov SI





	16.4.2014	23.4.2014	5.5.2014	14.5.2014
Št. ranljivih strežnikov SIX	1564	1332	961	861
Št. ranljivih strežnikov SI	934	758	518	451

si·cert

arnes

si·cert