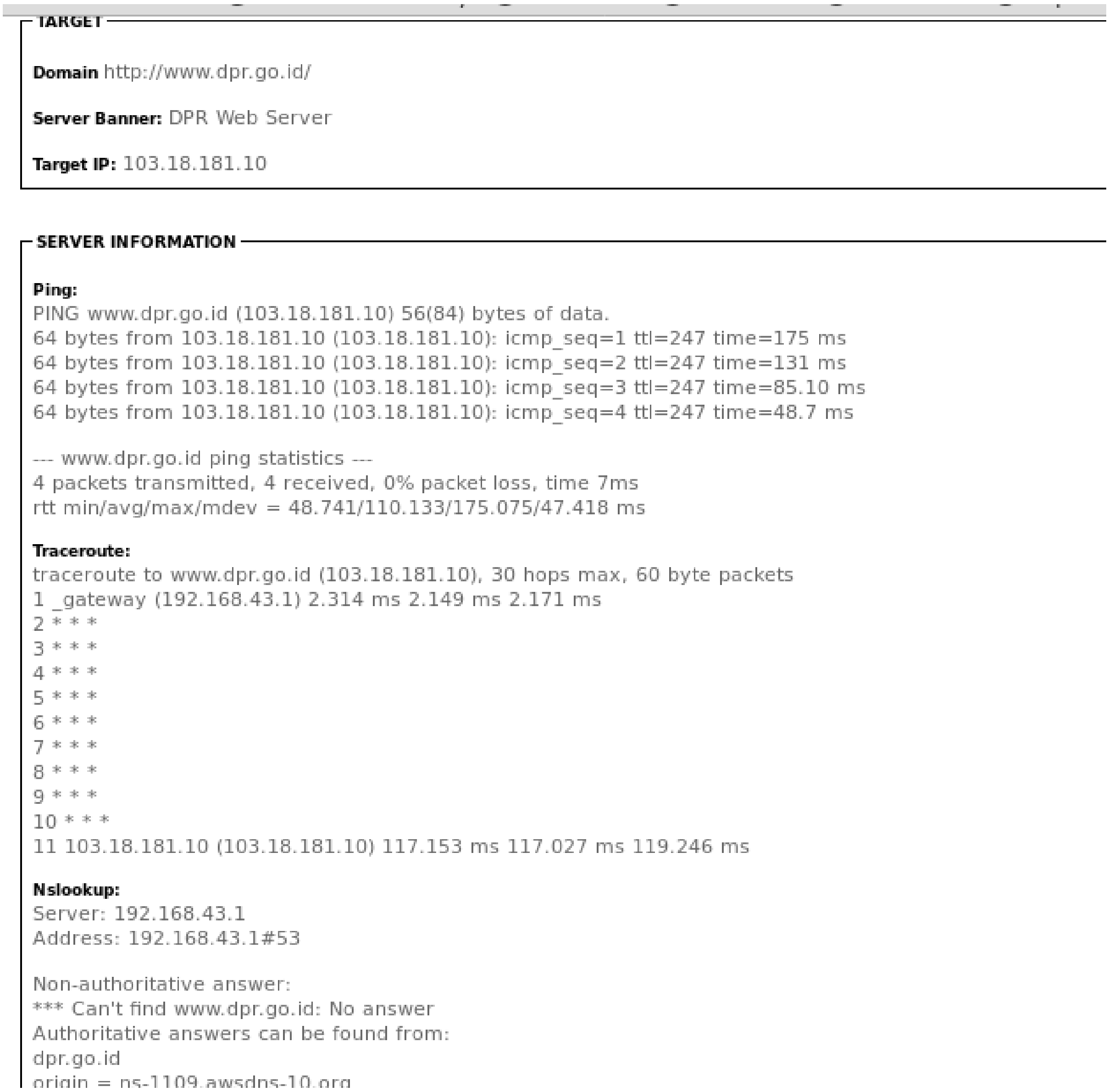
Nama : Pascal Adhi Kurnia Tarigan

NIM : 09011281520113

Website Pemerintahan

http://www.dpr.go.id/



TARGET

Domain http://www.dpr.go.id/

Server Banner: DPR Web Server

Target IP: 103.18.181.10

SERVER INFORMATION

Ping:

```
PING www.dpr.go.id (103.18.181.10) 56(84) bytes of data.
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=1 ttl=247 time=175 ms
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=2 ttl=247 time=131 ms
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=3 ttl=247 time=85.10 ms
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=4 ttl=247 time=48.7 ms

--- www.dpr.go.id ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 48.741/110.133/175.075/47.418 ms
```

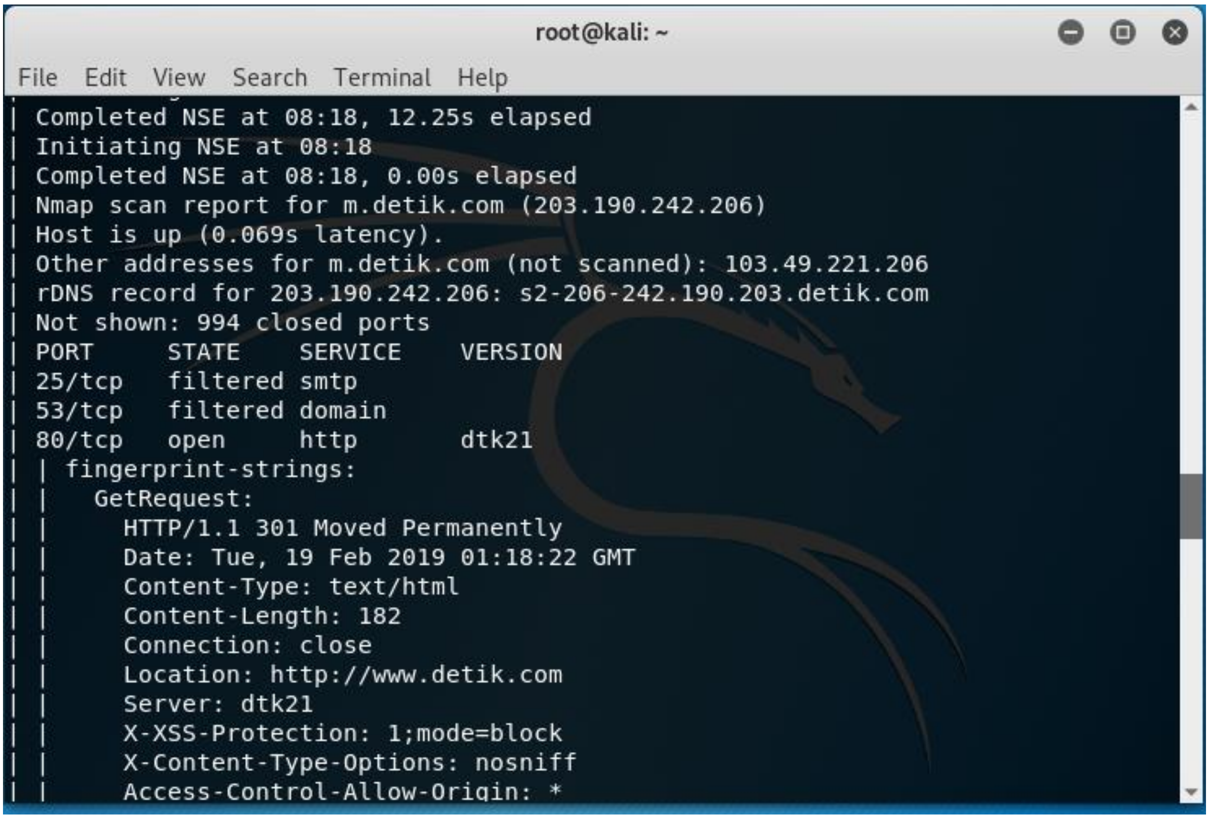
Traceroute:

```
traceroute to www.dpr.go.id (103.18.181.10), 30 hops max, 60 byte packets
1 _gateway (192.168.43.1) 2.314 ms 2.149 ms 2.171 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 103.18.181.10 (103.18.181.10) 117.153 ms 117.027 ms 119.246 ms
```

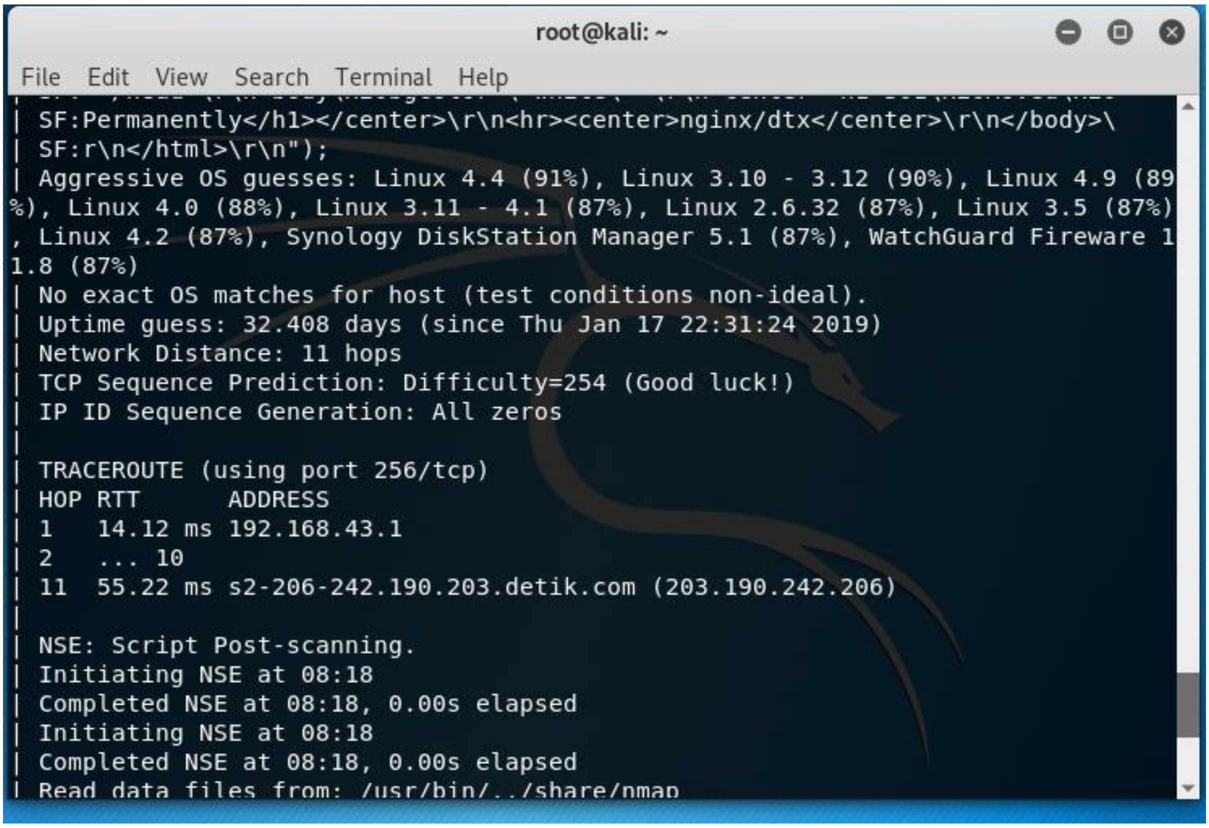
Nslookup:

```
Server: 192.168.43.1
Address: 192.168.43.1#53

Non-authoritative answer:
*** Can't find www.dpr.go.id: No answer
Authoritative answers can be found from:
dpr.go.id
origin = ns-1109.awsdns-10.org
```

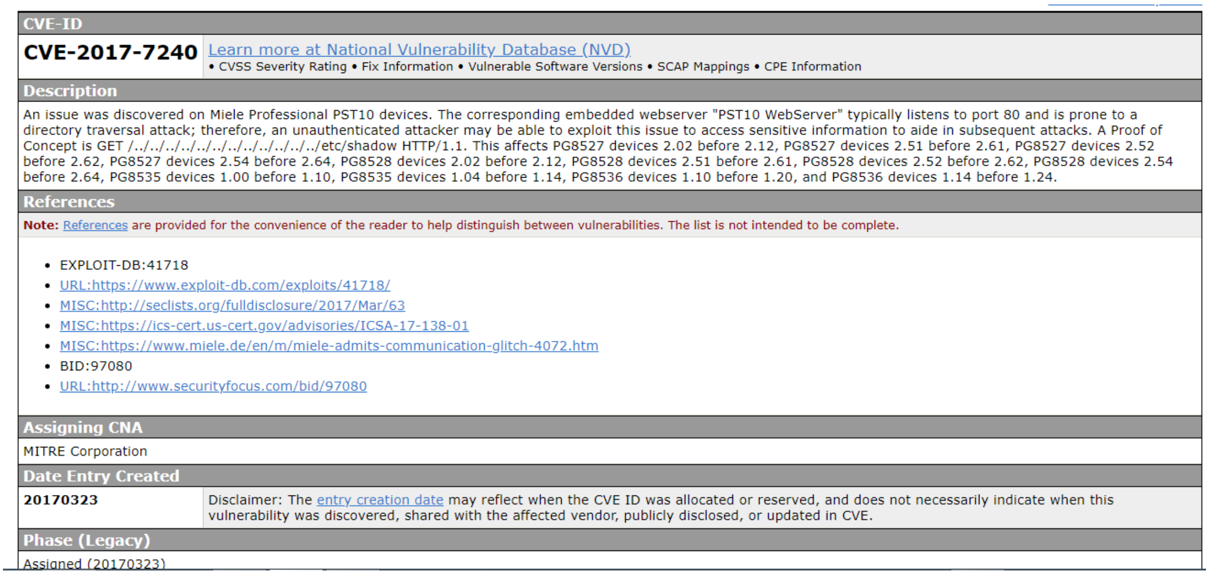


```
| Completed NSE at 08:18, 12.25s elapsed
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Nmap scan report for m.detik.com (203.190.242.206)
| Host is up (0.069s latency).
| Other addresses for m.detik.com (not scanned): 103.49.221.206
| rDNS record for 203.190.242.206: s2-206-242.190.203.detik.com
| Not shown: 994 closed ports
| PORT     STATE    SERVICE    VERSION
| 25/tcp   filtered smtp
| 53/tcp   filtered domain
| 80/tcp   open     http       dtk21
| | fingerprint-strings:
| |   GetRequest:
| |     HTTP/1.1 301 Moved Permanently
| |     Date: Tue, 19 Feb 2019 01:18:22 GMT
| |     Content-Type: text/html
| |     Content-Length: 182
| |     Connection: close
| |     Location: http://www.detik.com
| |     Server: dtk21
| |     X-XSS-Protection: 1;mode=block
| |     X-Content-Type-Options: nosniff
| |     Access-Control-Allow-Origin: *
```



```
| SF:Permanently</h1></center>\r\n<hr><center>nginx/dtx</center>\r\n</body>\
| SF:r\n</html>\r\n");
| Aggressive OS guesses: Linux 4.4 (91%), Linux 3.10 - 3.12 (90%), Linux 4.9 (89
%), Linux 4.0 (88%), Linux 3.11 - 4.1 (87%), Linux 2.6.32 (87%), Linux 3.5 (87%)
, Linux 4.2 (87%), Synology DiskStation Manager 5.1 (87%), WatchGuard Fireware 1
1.8 (87%)
| No exact OS matches for host (test conditions non-ideal).
| Uptime guess: 32.408 days (since Thu Jan 17 22:31:24 2019)
| Network Distance: 11 hops
| TCP Sequence Prediction: Difficulty=254 (Good luck!)
| IP ID Sequence Generation: All zeros
|
| TRACEROUTE (using port 256/tcp)
| HOP RTT      ADDRESS
| 1   14.12 ms 192.168.43.1
| 2   ... 10
| 11  55.22 ms s2-206-242.190.203.detik.com (203.190.242.206)
|
| NSE: Script Post-scanning.
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Read data files from: /usr/bin/../share/nmap
```

CVE (Common Vulnerabilities and Exposures)



CVE-ID

CVE-2017-7240 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An issue was discovered on Miele Professional PST10 devices. The corresponding embedded webserver "PST10 WebServer" typically listens to port 80 and is prone to a directory traversal attack; therefore, an unauthenticated attacker may be able to exploit this issue to access sensitive information to aide in subsequent attacks. A Proof of Concept is GET /../../../../../../../../../../../../etc/shadow HTTP/1.1. This affects PG8527 devices 2.02 before 2.12, PG8527 devices 2.51 before 2.61, PG8527 devices 2.52 before 2.62, PG8527 devices 2.54 before 2.64, PG8528 devices 2.02 before 2.12, PG8528 devices 2.51 before 2.61, PG8528 devices 2.52 before 2.62, PG8528 devices 2.54 before 2.64, PG8535 devices 1.00 before 1.10, PG8535 devices 1.04 before 1.14, PG8536 devices 1.10 before 1.20, and PG8536 devices 1.14 before 1.24.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:41718
- URL:https://www.exploit-db.com/exploits/41718/
- MISC:http://seclists.org/fulldisclosure/2017/Mar/63
- MISC:https://ics-cert.us-cert.gov/advisories/ICSA-17-138-01
- MISC:https://www.miele.de/en/m/miele-admits-communication-glitch-4072.htm
- BID:97080
- URL:http://www.securityfocus.com/bid/97080

Assigning CNA

MITRE Corporation

Date Entry Created

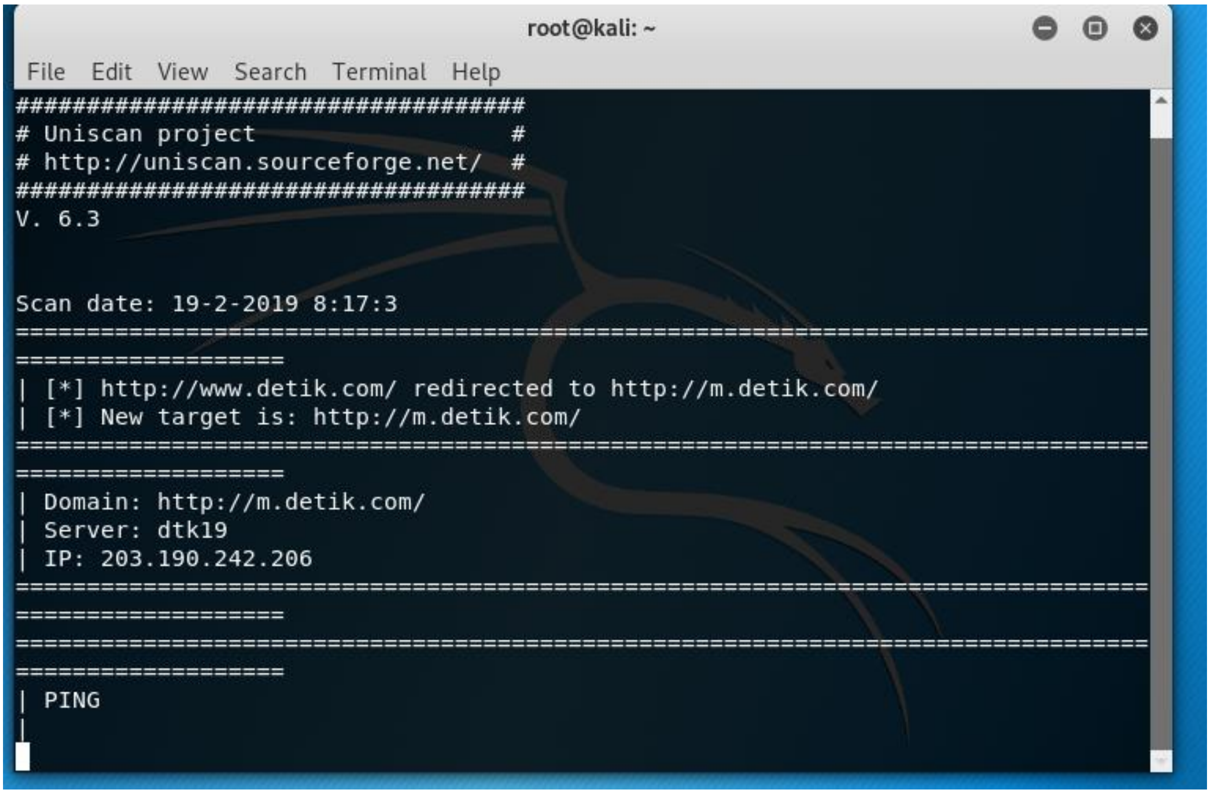
20170323 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20170323)

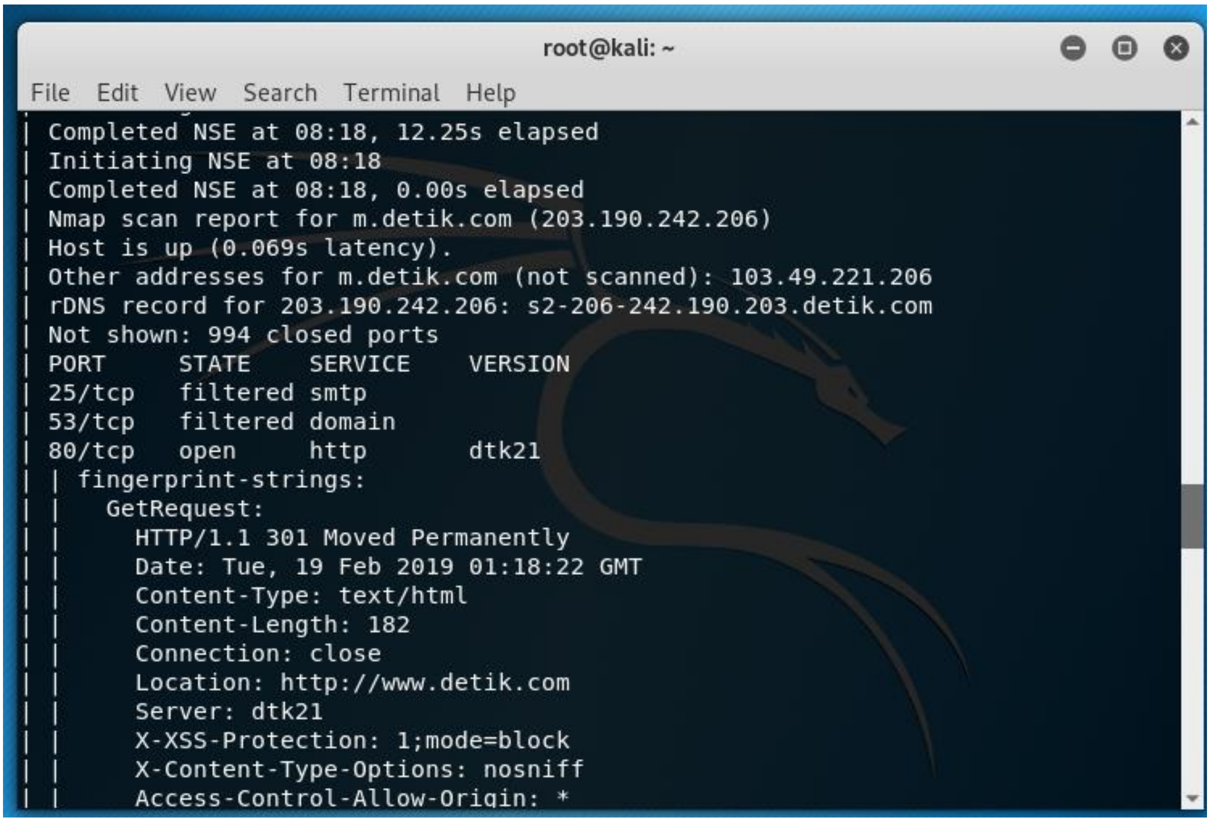
Website Dalam Negeri

https://www.detik.com

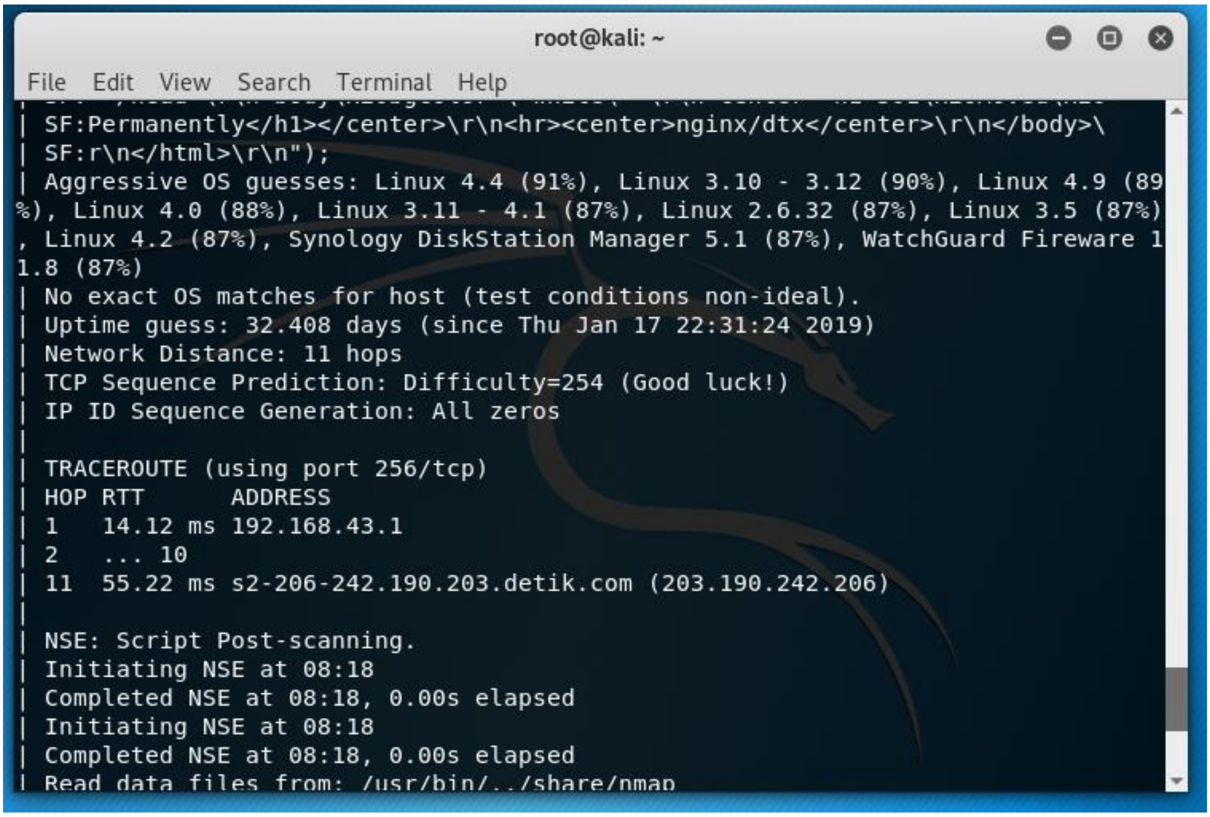


```
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 19-2-2019 8:17:3
================================================================================
===================
| [*] http://www.detik.com/ redirected to http://m.detik.com/
| [*] New target is: http://m.detik.com/
================================================================================
===================
| Domain: http://m.detik.com/
| Server: dtk19
| IP: 203.190.242.206
================================================================================
===================
================================================================================
===================
| PING
|
```

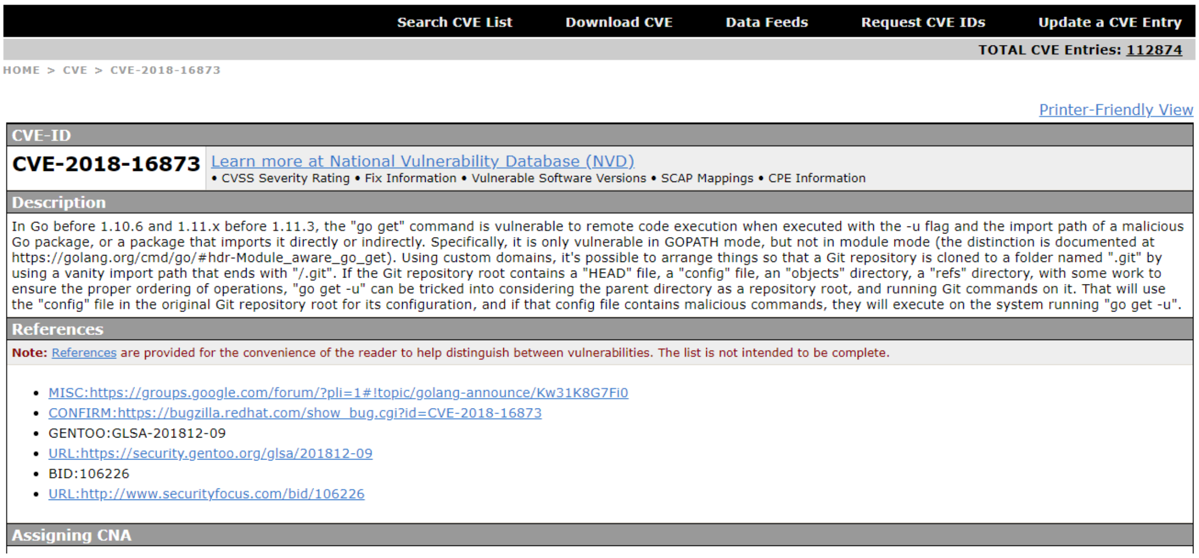


```
| Completed NSE at 08:18, 12.25s elapsed
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Nmap scan report for m.detik.com (203.190.242.206)
| Host is up (0.069s latency).
| Other addresses for m.detik.com (not scanned): 103.49.221.206
| rDNS record for 203.190.242.206: s2-206-242.190.203.detik.com
| Not shown: 994 closed ports
| PORT     STATE    SERVICE    VERSION
| 25/tcp   filtered smtp
| 53/tcp   filtered domain
| 80/tcp   open     http       dtk21
| | fingerprint-strings:
| |   GetRequest:
| |     HTTP/1.1 301 Moved Permanently
| |     Date: Tue, 19 Feb 2019 01:18:22 GMT
| |     Content-Type: text/html
| |     Content-Length: 182
| |     Connection: close
| |     Location: http://www.detik.com
| |     Server: dtk21
| |     X-XSS-Protection: 1;mode=block
| |     X-Content-Type-Options: nosniff
| |     Access-Control-Allow-Origin: *
```



```
| SF:Permanently</h1></center>\r\n<hr><center>nginx/dtx</center>\r\n</body>\
| SF:r\n</html>\r\n");
| Aggressive OS guesses: Linux 4.4 (91%), Linux 3.10 - 3.12 (90%), Linux 4.9 (89
%), Linux 4.0 (88%), Linux 3.11 - 4.1 (87%), Linux 2.6.32 (87%), Linux 3.5 (87%)
, Linux 4.2 (87%), Synology DiskStation Manager 5.1 (87%), WatchGuard Fireware 1
1.8 (87%)
| No exact OS matches for host (test conditions non-ideal).
| Uptime guess: 32.408 days (since Thu Jan 17 22:31:24 2019)
| Network Distance: 11 hops
| TCP Sequence Prediction: Difficulty=254 (Good luck!)
| IP ID Sequence Generation: All zeros
|
| TRACEROUTE (using port 256/tcp)
| HOP RTT      ADDRESS
| 1   14.12 ms 192.168.43.1
| 2   ... 10
| 11  55.22 ms s2-206-242.190.203.detik.com (203.190.242.206)
|
| NSE: Script Post-scanning.
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Read data files from: /usr/bin/../share/nmap
```

CVE (Common Vulnerabilities and Exposures)



TOTAL CVE Entries: 112874

CVE-ID

CVE-2018-16873 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

In Go before 1.10.6 and 1.11.x before 1.11.3, the "go get" command is vulnerable to remote code execution when executed with the -u flag and the import path of a malicious Go package, or a package that imports it directly or indirectly. Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at https://golang.org/cmd/go/#hdr-Module_aware_go_get). Using custom domains, it's possible to arrange things so that a Git repository is cloned to a folder named ".git" by using a vanity import path that ends with "/.git". If the Git repository root contains a "HEAD" file, a "config" file, an "objects" directory, a "refs" directory, with some work to ensure the proper ordering of operations, "go get -u" can be tricked into considering the parent directory as a repository root, and running Git commands on it. That will use the "config" file in the original Git repository root for its configuration, and if that config file contains malicious commands, they will execute on the system running "go get -u".

References

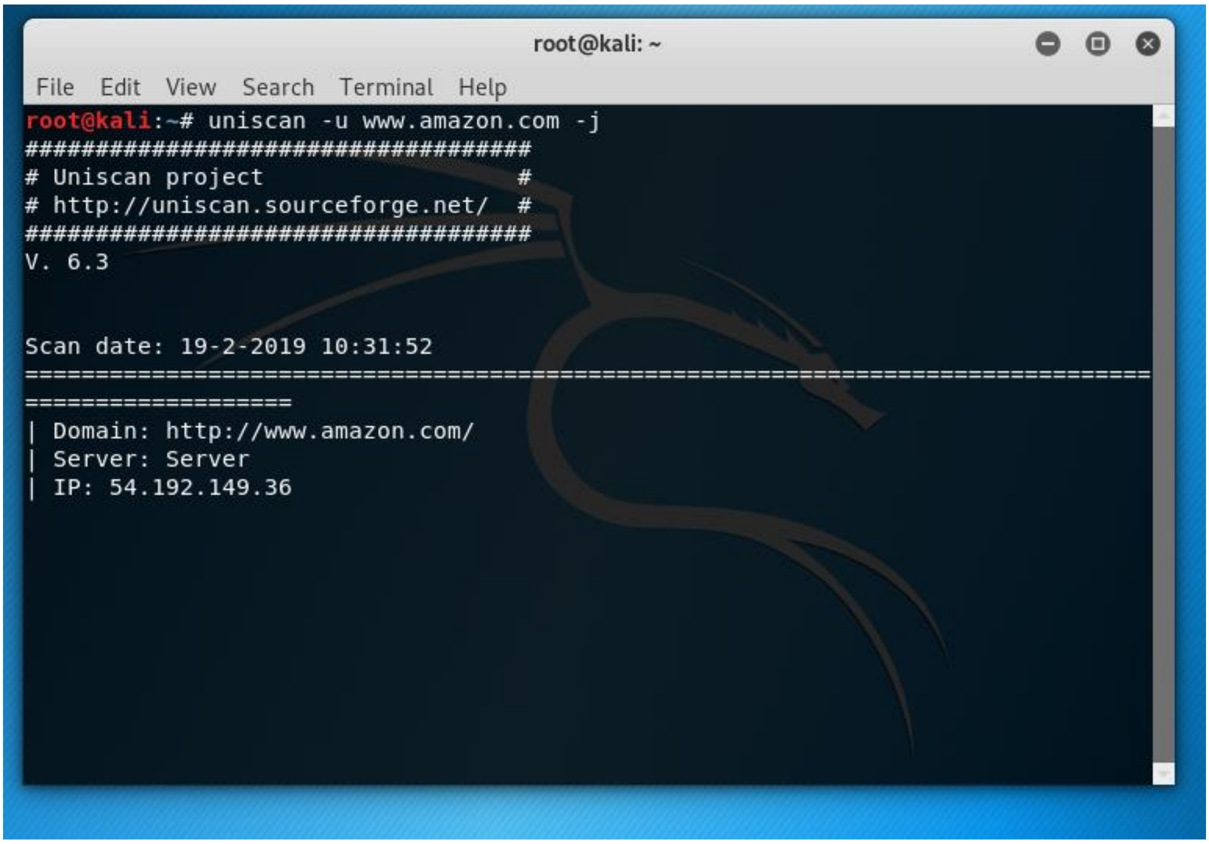
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://groups.google.com/forum/?pli=1#!topic/golang-announce/Kw31K8G7Fi0
- CONFIRM:https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16873
- GENTOO:GLSA-201812-09
- URL:https://security.gentoo.org/glsa/201812-09
- BID:106226
- URL:http://www.securityfocus.com/bid/106226

Assigning CNA

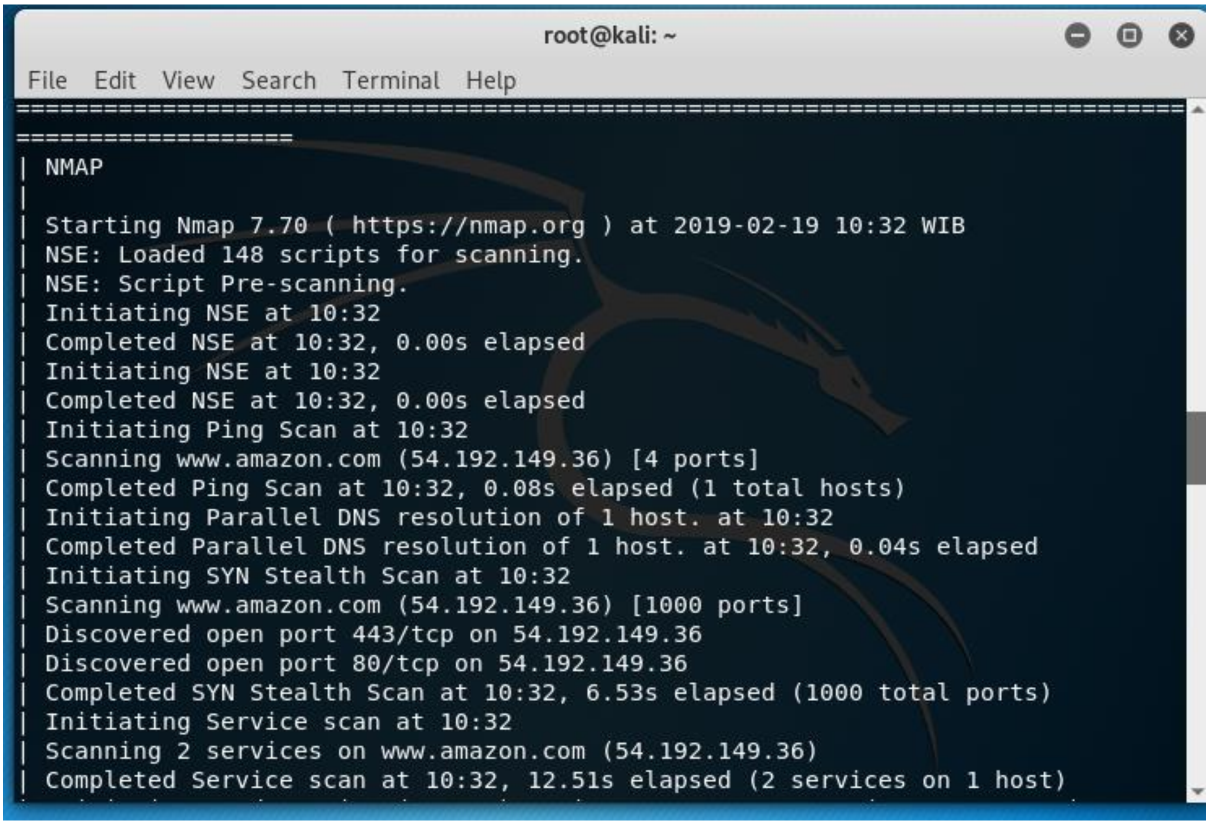
Website Luar negeri

https://www.amazon.com/

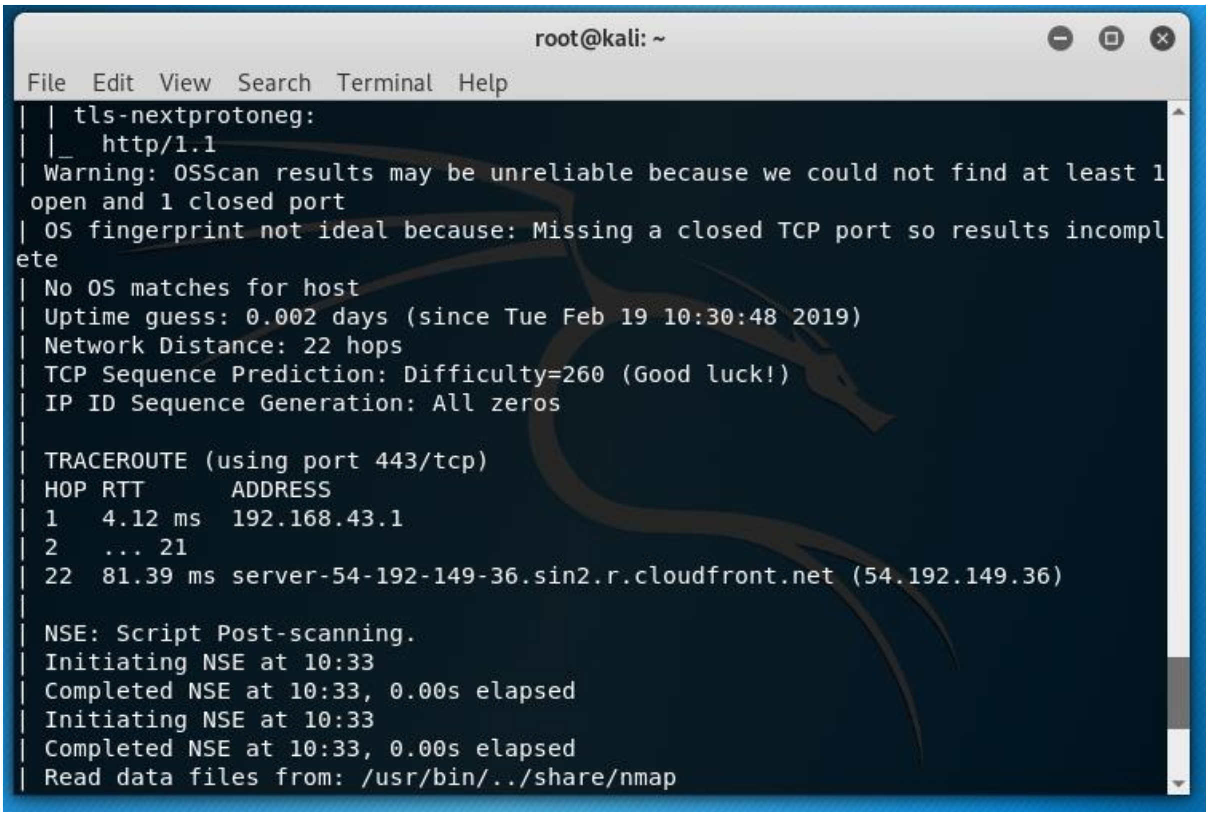


```
root@kali:~# uniscan -u www.amazon.com -j
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 19-2-2019 10:31:52
================================================================================
===================
| Domain: http://www.amazon.com/
| Server: Server
| IP: 54.192.149.36
```

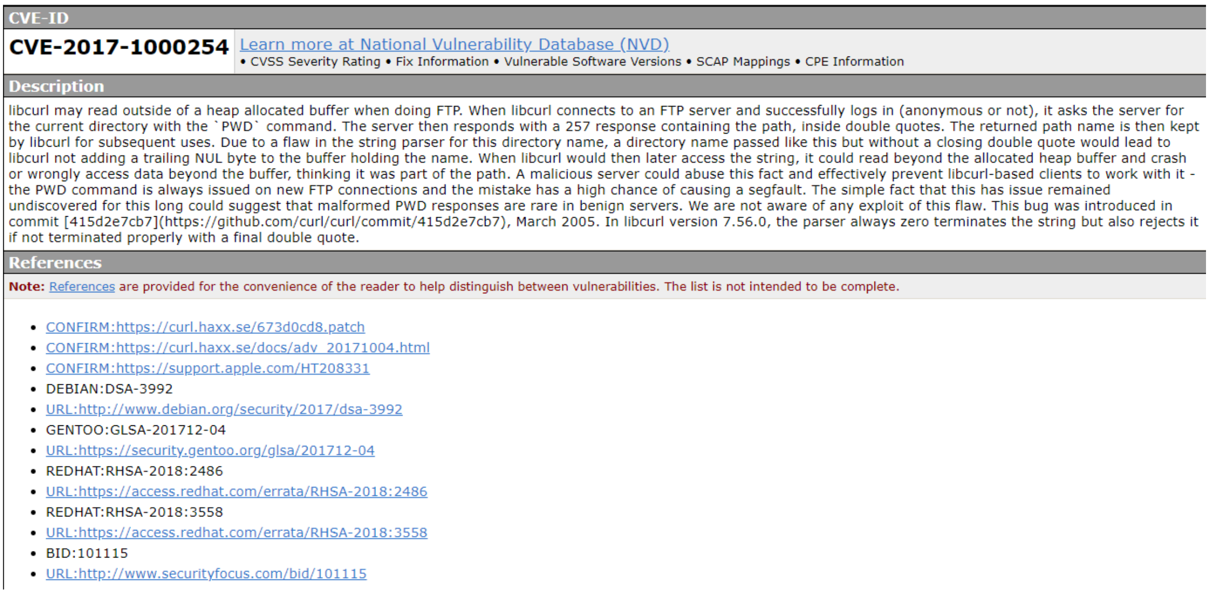


```
================================================================================
===================
| NMAP
|
| Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-19 10:32 WIB
| NSE: Loaded 148 scripts for scanning.
| NSE: Script Pre-scanning.
| Initiating NSE at 10:32
| Completed NSE at 10:32, 0.00s elapsed
| Initiating NSE at 10:32
| Completed NSE at 10:32, 0.00s elapsed
| Initiating Ping Scan at 10:32
| Scanning www.amazon.com (54.192.149.36) [4 ports]
| Completed Ping Scan at 10:32, 0.08s elapsed (1 total hosts)
| Initiating Parallel DNS resolution of 1 host. at 10:32
| Completed Parallel DNS resolution of 1 host. at 10:32, 0.04s elapsed
| Initiating SYN Stealth Scan at 10:32
| Scanning www.amazon.com (54.192.149.36) [1000 ports]
| Discovered open port 443/tcp on 54.192.149.36
| Discovered open port 80/tcp on 54.192.149.36
| Completed SYN Stealth Scan at 10:32, 6.53s elapsed (1000 total ports)
| Initiating Service scan at 10:32
| Scanning 2 services on www.amazon.com (54.192.149.36)
| Completed Service scan at 10:32, 12.51s elapsed (2 services on 1 host)
```



```
| | tls-nextprotoneg:
| |_   http/1.1
| Warning: OSScan results may be unreliable because we could not find at least 1
 open and 1 closed port
| OS fingerprint not ideal because: Missing a closed TCP port so results incompl
ete
| No OS matches for host
| Uptime guess: 0.002 days (since Tue Feb 19 10:30:48 2019)
| Network Distance: 22 hops
| TCP Sequence Prediction: Difficulty=260 (Good luck!)
| IP ID Sequence Generation: All zeros
|
| TRACEROUTE (using port 443/tcp)
| HOP RTT      ADDRESS
| 1   4.12 ms  192.168.43.1
| 2   ... 21
| 22  81.39 ms server-54-192-149-36.sin2.r.cloudfront.net (54.192.149.36)
|
| NSE: Script Post-scanning.
| Initiating NSE at 10:33
| Completed NSE at 10:33, 0.00s elapsed
| Initiating NSE at 10:33
| Completed NSE at 10:33, 0.00s elapsed
| Read data files from: /usr/bin/../share/nmap
```

CVE (Common Vulnerabilities and Exposures)



CVE-ID

CVE-2017-1000254 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

libcurl may read outside of a heap allocated buffer when doing FTP. When libcurl connects to an FTP server and successfully logs in (anonymous or not), it asks the server for the current directory with the `PWD` command. The server then responds with a 257 response containing the path, inside double quotes. The returned path name is then kept by libcurl for subsequent uses. Due to a flaw in the string parser for this directory name, a directory name passed like this but without a closing double quote would lead to libcurl not adding a trailing NUL byte to the buffer holding the name. When libcurl would then later access the string, it could read beyond the allocated heap buffer and crash or wrongly access data beyond the buffer, thinking it was part of the path. A malicious server could abuse this fact and effectively prevent libcurl-based clients to work with it - the PWD command is always issued on new FTP connections and the mistake has a high chance of causing a segfault. The simple fact that this has issue remained undiscovered for this long could suggest that malformed PWD responses are rare in benign servers. We are not aware of any exploit of this flaw. This bug was introduced in commit [415d2e7cb7](https://github.com/curl/curl/commit/415d2e7cb7), March 2005. In libcurl version 7.56.0, the parser always zero terminates the string but also rejects it if not terminated properly with a final double quote.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://curl.haxx.se/673d0cd8.patch
- CONFIRM:https://curl.haxx.se/docs/adv_20171004.html
- CONFIRM:https://support.apple.com/HT208331
- DEBIAN:DSA-3992
- URL:http://www.debian.org/security/2017/dsa-3992
- GENTOO:GLSA-201712-04
- URL:https://security.gentoo.org/glsa/201712-04
- REDHAT:RHSA-2018:2486
- URL:https://access.redhat.com/errata/RHSA-2018:2486
- REDHAT:RHSA-2018:3558
- URL:https://access.redhat.com/errata/RHSA-2018:3558
- BID:101115
- URL:http://www.securityfocus.com/bid/101115