Network Vulnerabilities

VULNERABILITY MANAGEMENT

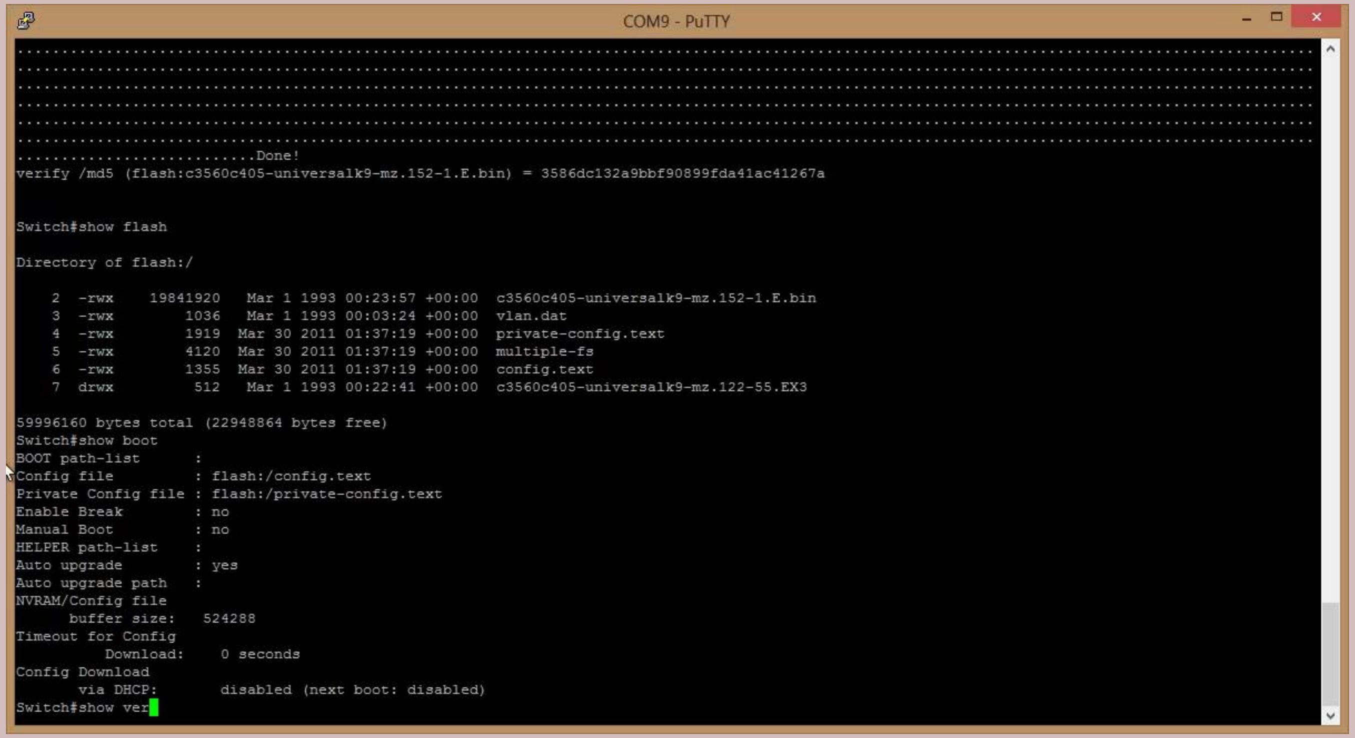
Network Vulnerabilities

- Missing Firmware Updates
- SSL and TLS Issues
- Domain Name Service (DNS) Issues
- Internal IP Disclosure
- Virtual Private Network (VPN) Issues

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Missing Firmware Updates

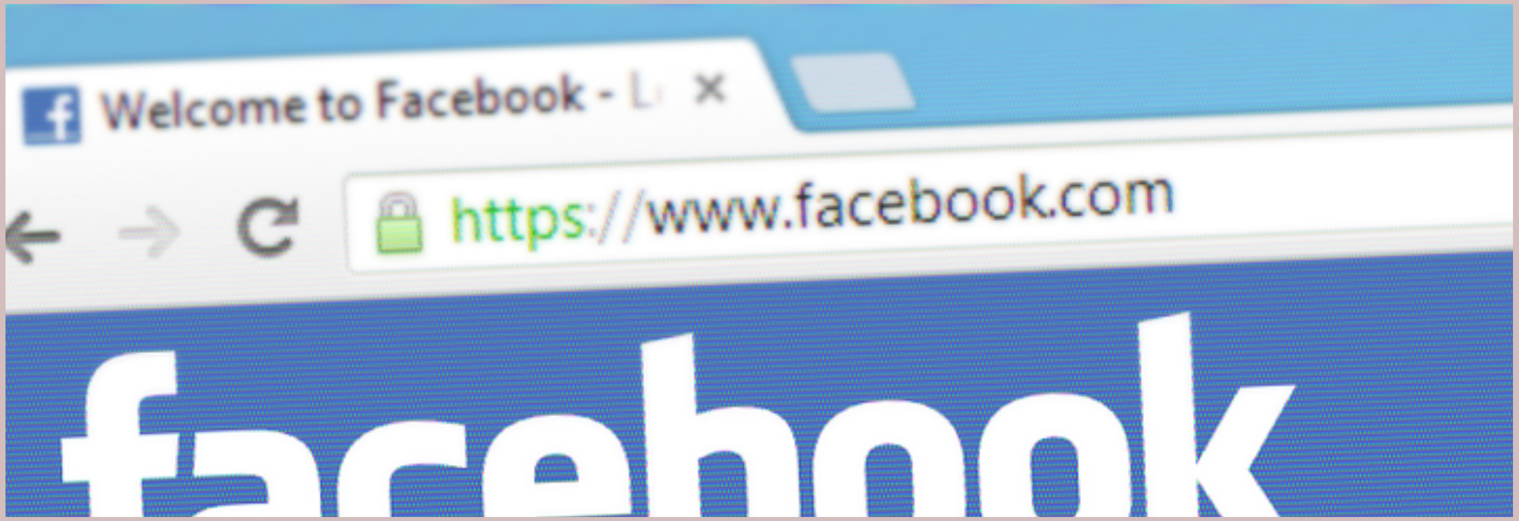
- Network devices rely on firmware for their operating systems
- Firmware needs patching and upgrades



```
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...................................................................................................................................................
...........................Done!
verify /md5 (flash:c3560c405-universalk9-mz.152-1.E.bin) = 3586dc132a9bbf90899fda41ac41267a


Switch#show flash

Directory of flash:/

    2  -rwx    19841920   Mar 1 1993 00:23:57 +00:00  c3560c405-universalk9-mz.152-1.E.bin
    3  -rwx        1036   Mar 1 1993 00:03:24 +00:00  vlan.dat
    4  -rwx        1919  Mar 30 2011 01:37:19 +00:00  private-config.text
    5  -rwx        4120  Mar 30 2011 01:37:19 +00:00  multiple-fs
    6  -rwx        1355  Mar 30 2011 01:37:19 +00:00  config.text
    7  drwx         512   Mar 1 1993 00:22:41 +00:00  c3560c405-universalk9-mz.122-55.EX3

59996160 bytes total (22948864 bytes free)
Switch#show boot
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
NVRAM/Config file
      buffer size:   524288
Timeout for Config
          Download:    0 seconds
Config Download
       via DHCP:       disabled (next boot: disabled)
Switch#show ver
```

SSL and TLS Issues

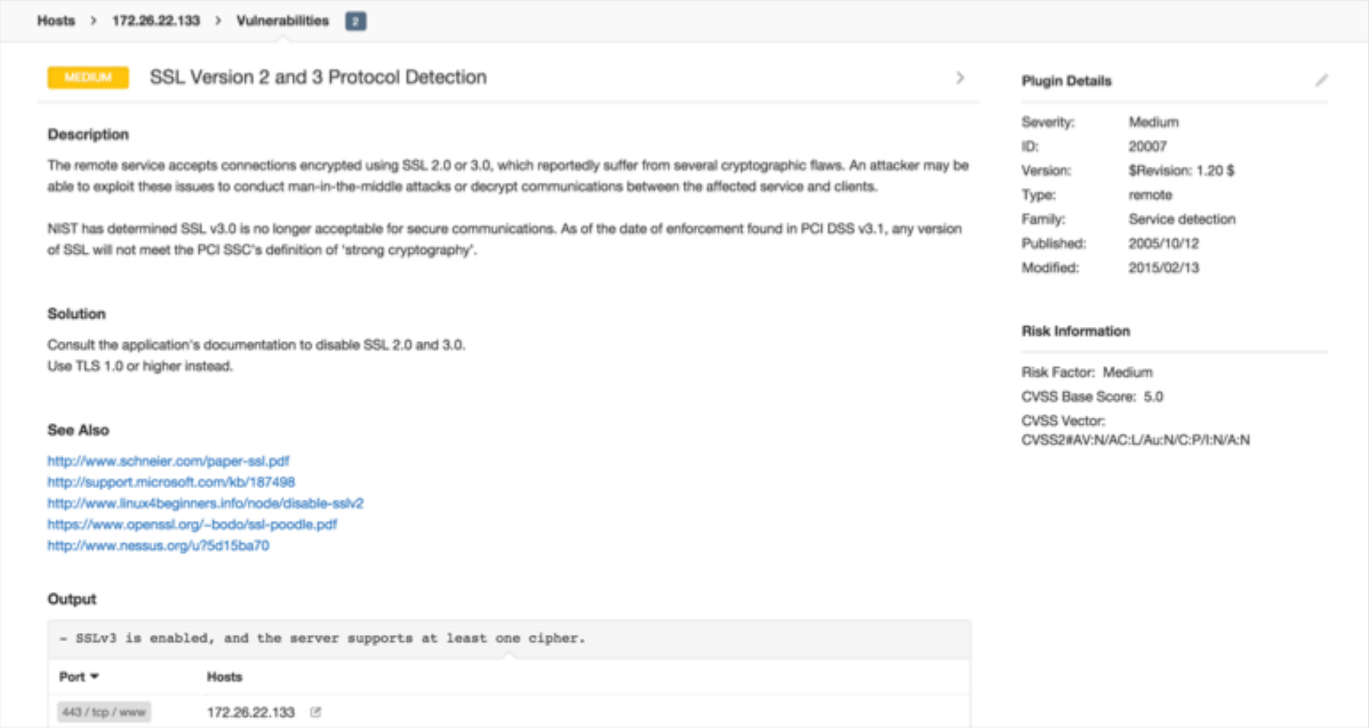
- Secure Socket Layer (SSL) and Transport Layer Security (TLS) are designed to secure information sent over the internet (such as HTTPS)



Outdated SSL/TLS Versions

- SSL is insecure and shouldn’t be used

- Admins should disable support for older versions (SSL and TLS before v1.2)



SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 or 3.0, which reportedly suffer from several cryptographic flaws. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

NIST has determined SSL v3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.0 or higher instead.

See Also

http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70

Output

```
- SSLv3 is enabled, and the server supports at least one cipher.
```

Port ▾	Hosts
443 / tcp / www	172.26.22.133

Plugin Details

Severity:	Medium
ID:	20007
Version:	$Revision: 1.20 $
Type:	remote
Family:	Service detection
Published:	2005/10/12
Modified:	2015/02/13

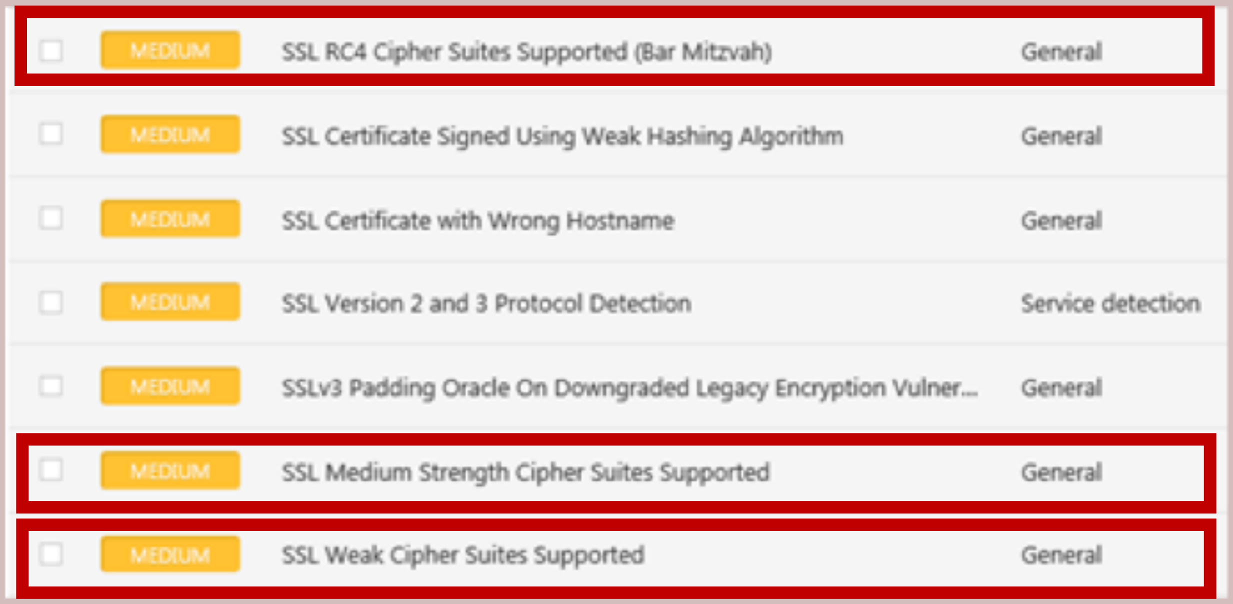
Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Insecure Cipher Use

- SSL/TLS are only the protocol used, not the cipher

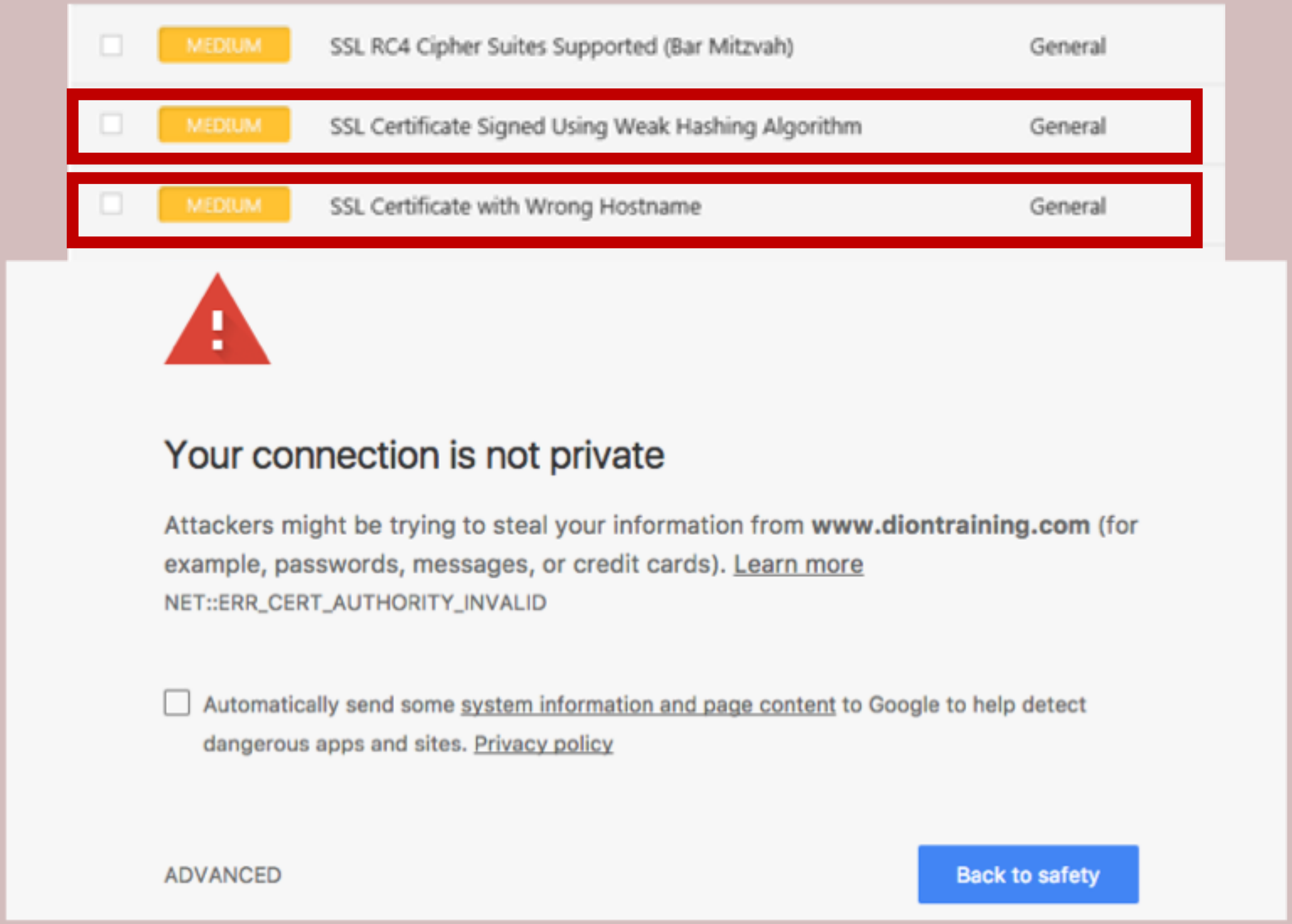
- Cipher is the encryption algorithm



□	MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General
□	MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General
□	MEDIUM	SSL Certificate with Wrong Hostname	General
□	MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection
□	MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulner...	General
□	MEDIUM	SSL Medium Strength Cipher Suites Supported	General
□	MEDIUM	SSL Weak Cipher Suites Supported	General

SSL/TLS Certificate Problems

- Certificates identify servers and exchange the encryption keys



□	MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General
□	MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General
□	MEDIUM	SSL Certificate with Wrong Hostname	General

Your connection is not private

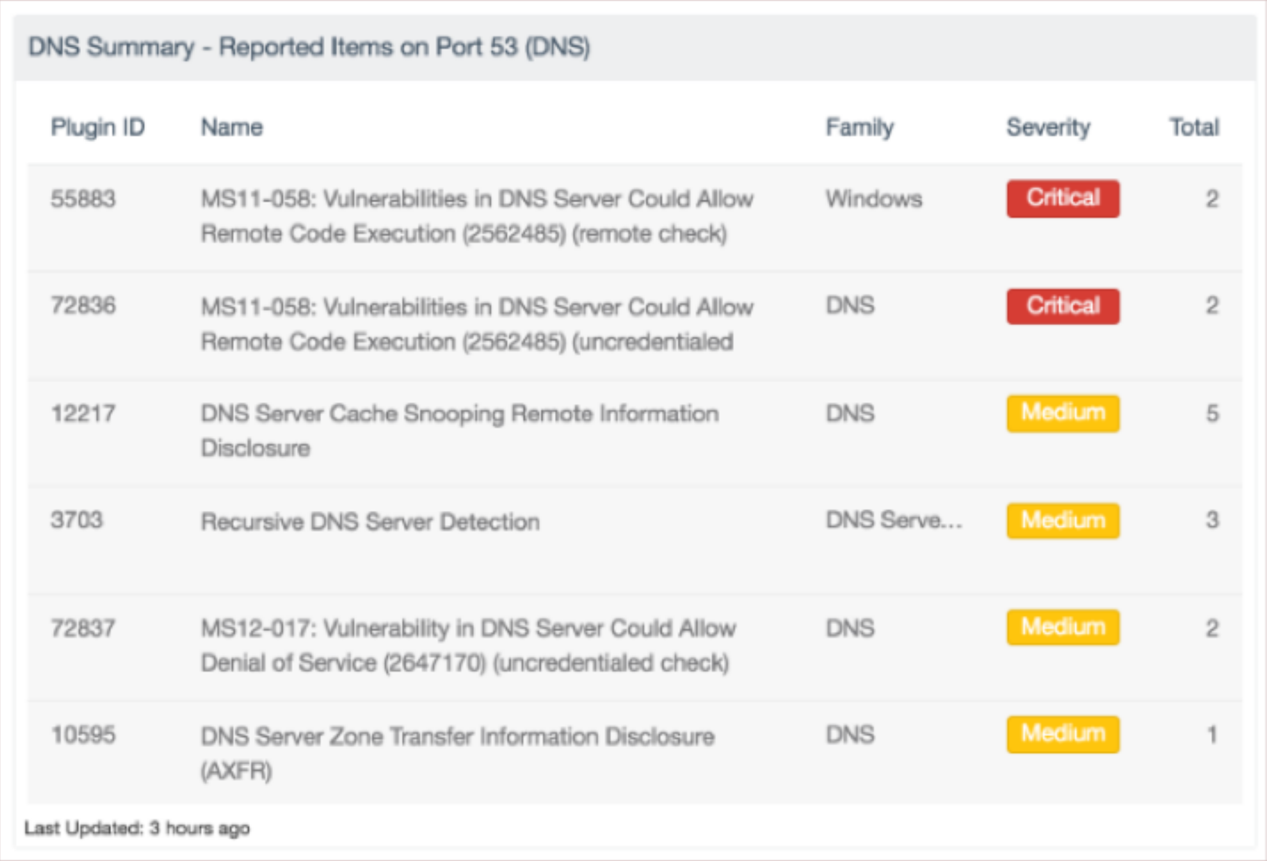
Attackers might be trying to steal your information from **www.diontraining.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

DNS Issues

- DNS servers are victims of reconnaissance and other attacks



DNS Summary - Reported Items on Port 53 (DNS)

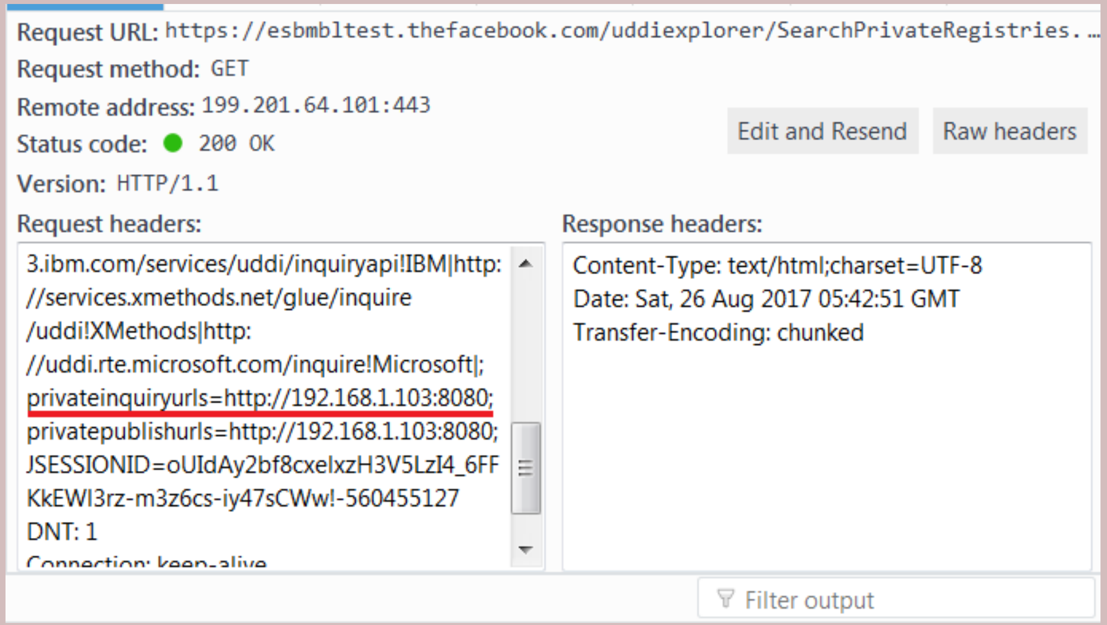
Plugin ID	Name	Family	Severity	Total
55883	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (remote check)	Windows	Critical	2
72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed	DNS	Critical	2
12217	DNS Server Cache Snooping Remote Information Disclosure	DNS	Medium	5
3703	Recursive DNS Server Detection	DNS Serve...	Medium	3
72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)	DNS	Medium	2
10595	DNS Server Zone Transfer Information Disclosure (AXFR)	DNS	Medium	1

Last Updated: 3 hours ago

Internal IP Disclosure

- Networks that use NAT attempt to hide their internal IP structure

- Information could be leaked in headers if a server isn't configured properly



Request URL: https://esbmbltest.thefacebook.com/uddiexplorer/SearchPrivateRegistries. …
Request method: GET
Remote address: 199.201.64.101:443
Status code: ● 200 OK
Version: HTTP/1.1

Request headers:

```
3.ibm.com/services/uddi/inquiryapi!IBM|http:
//services.xmethods.net/glue/inquire
/uddi!XMethods|http:
//uddi.rte.microsoft.com/inquire!Microsoft|;
privateinquiryurls=http://192.168.1.103:8080;
privatepublishurls=http://192.168.1.103:8080;
JSESSIONID=oUIdAy2bf8cxelxzH3V5LzI4_6FF
KkEWI3rz-m3z6cs-iy47sCWw!-560455127
DNT: 1
Connection: keep-alive
```

Response headers:

```
Content-Type: text/html;charset=UTF-8
Date: Sat, 26 Aug 2017 05:42:51 GMT
Transfer-Encoding: chunked
```

Sourced from https://datarift.blogspot.com/p/facebook-internal-ip-disclosure.html

VPN Issues

- VPNs consist of application protocols and SSL/TLS encrypted tunnels
- Configuration issues and missing firmware patches can also affect VPNs