Security Lab 7 - Crypto & Web Applications

Ana Herrera Flores

Fundamentals of Information Security: Cybersecurity (88252)

Exercise 1 – Nessus Scan – Web Server Vulnerabilities

1. What is the Severity?

Critical.

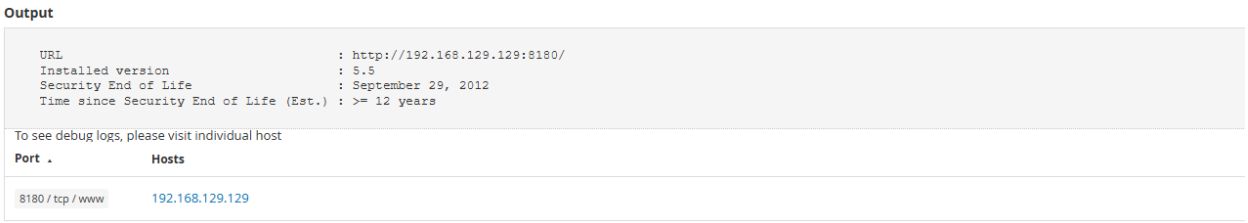
2. What is the Description?

Apache Tomcat is less than or equal to 5.5x, and it is no longer maintained by its vendor.

3. What is the Solution to eliminate the threat?

Upgrade the version.

4. What was the Output? (Diagnostic Info)



As we can see the version is 5.5 and it stopped being maintained on September 29, 2012.

5. What Port was the problem?

Port 8180.

6. What additional information is available? (See Also)

https://tomcat.apache.org/tomcat-55-eol.html

Exercise 2 – Nessus Scan – Application Server Vulnerabilities

1. What is the Severity?

High

2. What is the Description?

The PHP on the remote web server contains a flaw that could allow a remote attacker to send commands as part of a query string.

3. What is the Solution to eliminate the threat?

Upgrade Lotus Foundations or PHP to later versions.

4. What was the Output? (Diagnostic Info)

Nessus executed this request to verify the issue.

5. What Port was the problem?

Port 80.

6. What additional information is available? (See Also)

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

http://www.php.net/archive/2012.php#id2012-05-08-1

http://www.php.net/ChangeLog-5.php#5.3.13

http://www.php.net/ChangeLog-5.php#5.4.3

http://www.nessus.org/u?80589ce8

https://www-304.ibm.com/support/docview.wss?uid=swg21620314

Exercise 3 – Nessus Scan – Database Server Vulnerabilities

1.What is the Severity?

Info.

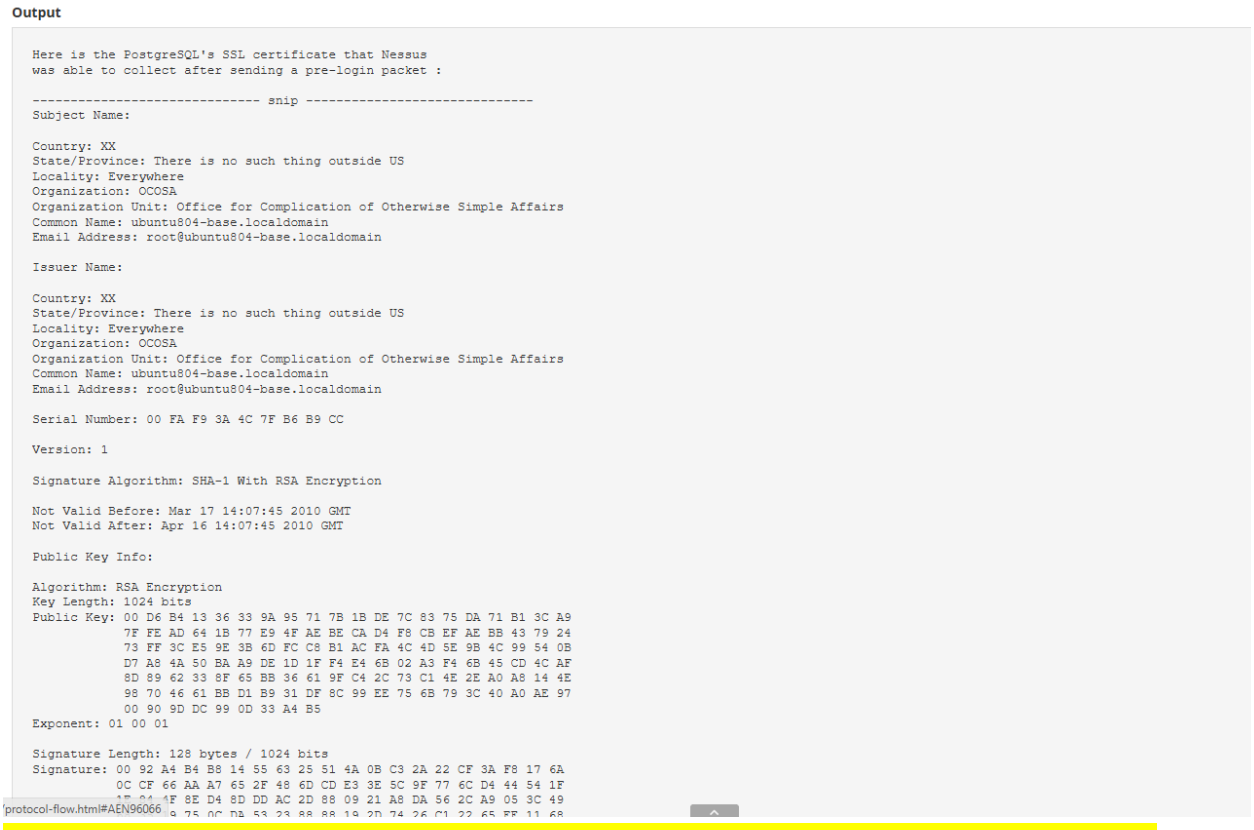
2. What is the Description?

The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from cleartext to encrypted communications channel.

3. What is the Solution to eliminate the threat?

No solution, just info.

4. What was the Output? (Diagnostic Info)



Output

```
Here is the PostgreSQL's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           [illegible] 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           [illegible]
```

'protocol-flow.html#AEN96066

Nessus was able to obtain the PostgreSQL's SSL certificate after sending a pre-login packet.

5. What Port was the problem?

Port 5432.

6. What additional information is available? (See Also)

No additional info.

Exercise 4 – Nessus Scan – SSL/TLS Vulnerabilities

1.What is the Severity?

Medium.

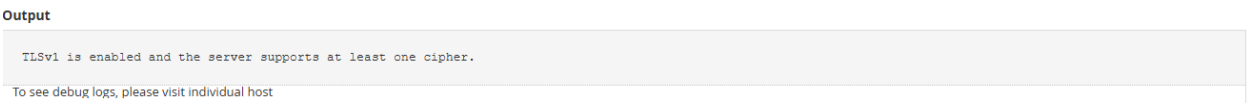
2. What is the Description?

Use of the TLS 1.0 which is an older version and has cryptographic design flaws.

3. What is the Solution to eliminate the threat?

Enable support for TLS 1.2 and 1.3, and disabled support for TLS 1.0.

4. What was the Output? (Diagnostic Info)



We can see the version of TLS.

5. What Port was the problem?

Port 5432

Port 25.

6. What additional information is available? (See Also)

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00