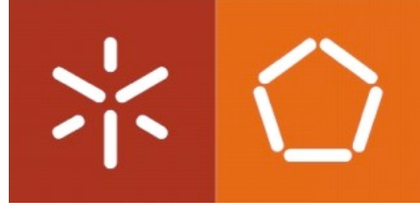
Universidade do Minho
Departamento de Informática



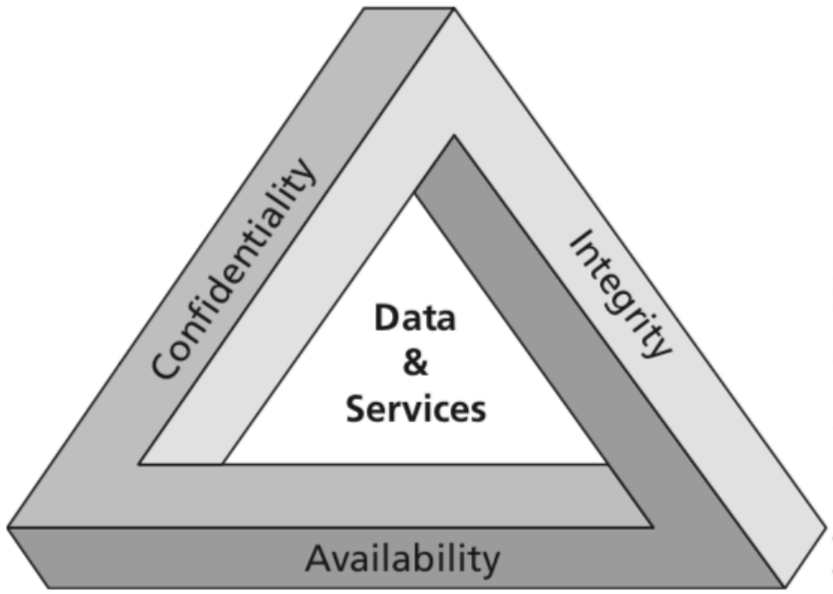
Tecnologia de Segurança

João Marco Silva
joaomarco@di.uminho.pt

Setembro, 2019

Concepts

- What is information security?
  - the protection of information and its critical elements, including the systems and hardware used to process, store, and transmit the information*.



The C.I.A. triangle

* Source: The Committee on National Security Systems (CNSS)

Concepts

- Confidentiality
    - ensures that only users/systems with the rights and privileges to access information are able to do so
- Integrity
    - ensures the authenticity of information
        - involves maintaining consistency, accuracy, and trustworthiness of data over its entire life cycle
- Availability
    - ensures authorized users/systems to access information without interference or obstruction

Concepts

- Additional key concepts
  - Asset: the resource being protected
  - Attack: intentional or unintentional act that can damage or otherwise compromise information and the systems that support it
  - Exploit: a technique used to compromise a system
  - Exposure: a condition or state of being exposed. It exists when a vulnerability is known to an attacker

Concepts

- Additional key concepts
  - Risk: the probability of an unwanted occurrence
  - Threat: a category of objects, people, or other entities that represents a danger to an asset
  - Vulnerability: a weakness or fault in a system or protection mechanism that opens it to attack or damage

Vulnerabilities

Do you know all the vulnerabilities your personal system is exposed to, right now?

Vulnerabilities

Kernel components

The most severe vulnerability in this section could enable a local malicious application to execute arbitrary code within the context of a privileged process.

CVE	References	Type	Severity	Component
CVE-2018-20669	A-135368228*	EoP	High	i915 driver
CVE-2019-2181	A-130571081 Upstream kernel	EoP	High	Binder driver

Android’s security update - September, 2019

Vulnerabilities

- A closer look - CVE-2017-18249

CVE-2017-18249 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

QUICK INFO

CVE Dictionary Entry:
CVE-2017-18249
NVD Published Date:
03/26/2018
NVD Last Modified:
08/08/2018

Current Description

The add_free_nid function in fs/f2fs/node.c in the Linux kernel before 4.12 does not properly track an allocated nid, which allows local users to cause a denial of service (race condition) or possibly have unspecified other impact via concurrent threads.

Source: MITRE
Description Last Modified: 03/26/2018

Vulnerabilities

- A closer look - CVE-2017-18249

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 7.0 HIGH

Vector: AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)

Impact Score: 5.9

Exploitability Score: 1.0

Attack Vector (AV): Local
Attack Complexity (AC): High
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:

Base Score: 4.4 MEDIUM

Vector: (AV:L/AC:M/Au:N/C:P/I:P/A:P) (V2 legend)

Impact Subscore: 6.4

Exploitability Subscore: 3.4

Access Vector (AV): Local
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

CVSS - Common Vulnerability Scoring System (https://goo.gl/iwgbCz)

Vulnerabilities

- CVE - Common Vulnerabilities and Exposures
  - a list of standardized names for vulnerabilities and other information related to publicly known security exposures
  - CVE is maintained by MITRE Corporation which is also responsible for moderating the Editorial Board
    - *cve.mitre.org*

Vulnerabilities

- Vulnerabilities databases
  - National Vulnerability Database - NVD
    - National Institute of Standards and Technology
    - nvd.nist.gov
  - MITRE
    - cve.mitre.org
  - CVE details
    - www.cvedetails.com
  - Rapid7
    - www.rapid7.com/db/vulnerabilities

Exploits

CVE-2016-2107 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

QUICK INFO

CVE Dictionary Entry:
CVE-2016-2107
NVD Published Date:
05/04/2016
NVD Last Modified:
07/18/2018

Description

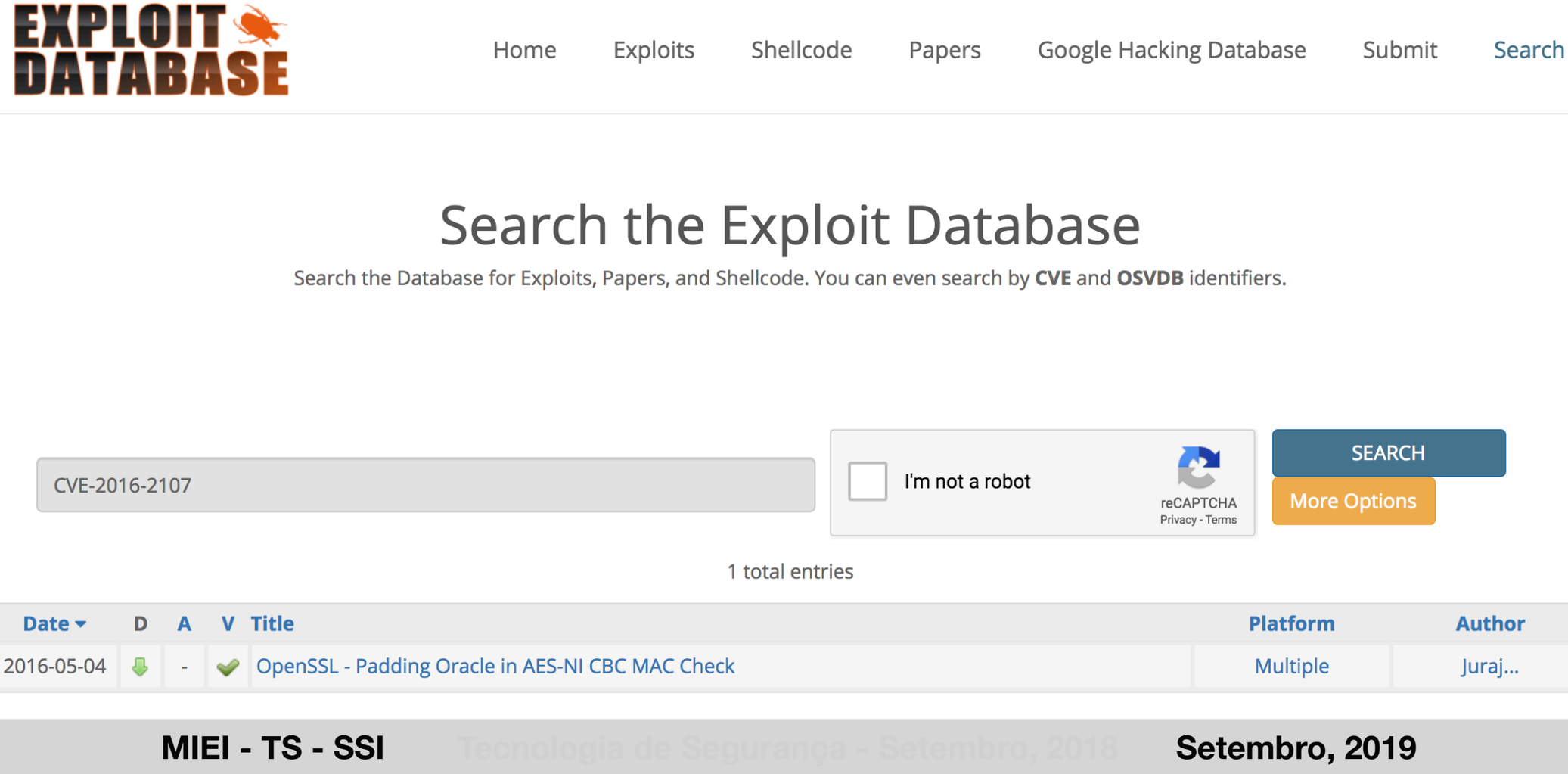
The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.

Source: MITRE
Description Last Modified: 04/03/2017

OpenSSL vulnerability
Intel Advanced Encryption - New Instructions (AES-NI)

Exploits

- Exploit Database - Exploit-DB
  - www.exploit-db.com



Exploits

OpenSSL - Padding Oracle in AES-NI CBC MAC Check

EDB-ID: 39768	**Author**: Juraj Somorovsky	**Published**: 2016-05-04
CVE: CVE-2016-2107	**Type**: Dos	**Platform**: Multiple
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified: ✔	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit

Next Exploit »

```
Source: http://web-in-security.blogspot.ca/2016/05/curious-padding-oracle-in-openssl-cve.html

TLS-Attacker:
https://github.com/RUB-NDS/TLS-Attacker
https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploits/39768.zip


You can use TLS-Attacker to build a proof of concept and test your implementation. You just start TLS-Attacker as follows:
java -jar TLS-Attacker-1.0.jar client -workflow_input rsa-overflow.xml -connect $host:$port

The xml configuration file (rsa-overflow.xml) looks then as follows:
```

Cipher Block Chaining - Message Authentication Code (**CBC-MAC**)

Exploits

- Scanning a server

```
Joaos-MacBook-Pro-6:~ joaomarcosilva$ nmap -sV -Pn --script ssl-enum-ciphers -p 443 www.ine.pt
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-21 11:17 WEST
Nmap scan report for www.ine.pt (193.192.10.184)
Host is up (0.0082s latency).
rDNS record for 193.192.10.184: portal-rpe01.ine.pt

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http nginx
|_http-server-header: nginx
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
```

NMAP scanning

Hands on

- What about **phpMyAdmin**?