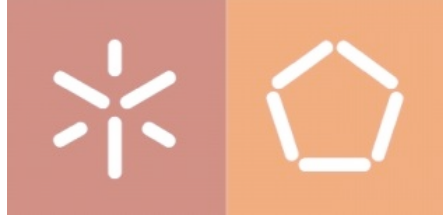




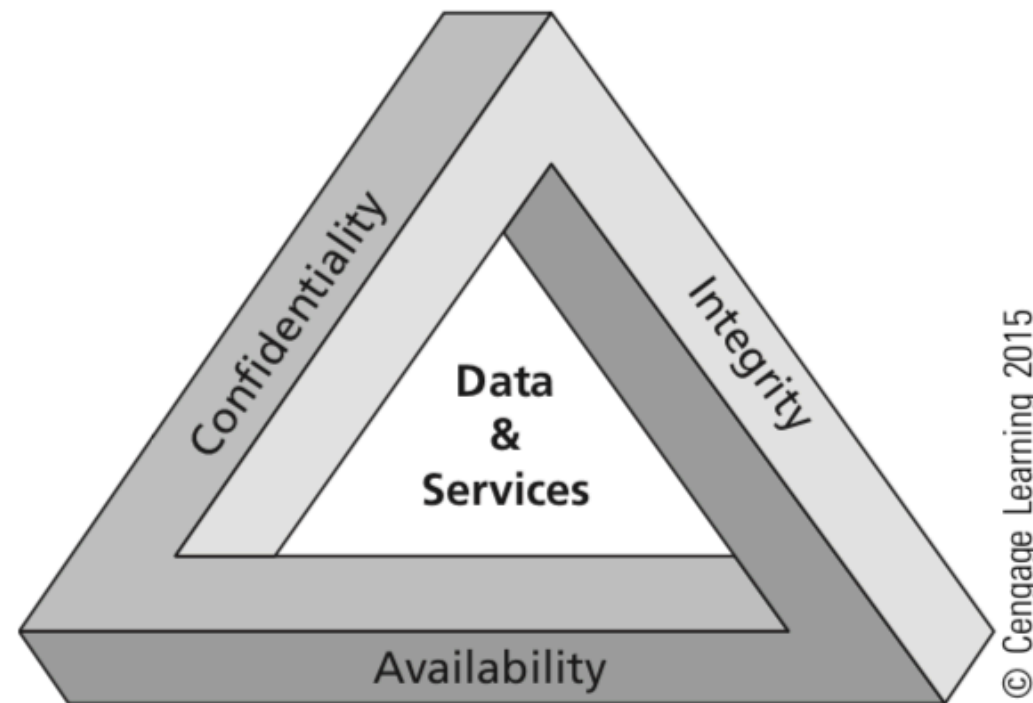
# Segurança de Sistemas Informáticos

João Marco Silva  
[joaomarco@di.uminho.pt](mailto:joaomarco@di.uminho.pt)

# Concepts



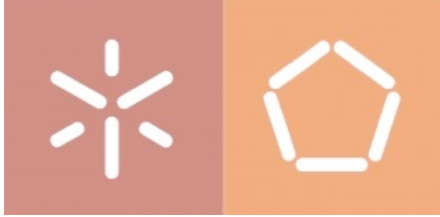
- What is information security?
- the protection of information and its critical elements, including the systems and hardware used to process, store, and transmit the information\*.



**The C.I.A. triangle**

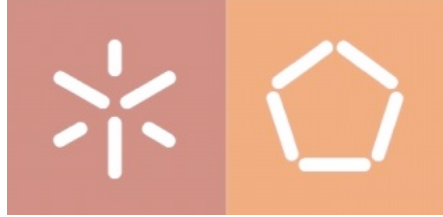
\* Source: The Committee on National Security Systems (CNSS)

# Concepts



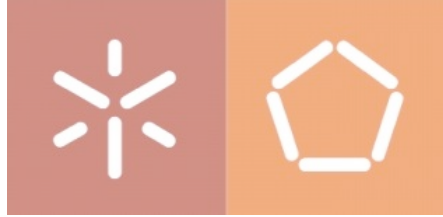
- Confidentiality
  - ensures that only users/systems with the rights and privileges to access information are able to do so
- Integrity
  - ensures the authenticity of information
    - involves maintaining consistency, accuracy, and trustworthiness of data over its entire life cycle
- Availability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

# Concepts



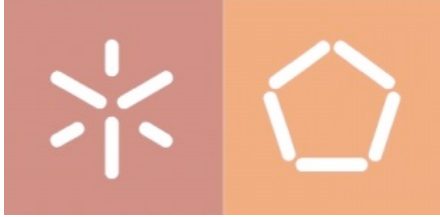
- Additional key concepts
  - Asset: the resource being protected
  - Attack: intentional or unintentional act that can damage or otherwise compromise information and the systems that support it
  - Exploit: a technique used to compromise a system
  - Exposure: a condition or state of being exposed.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



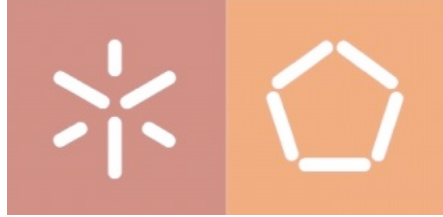
## Kernel components

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 <a href="#">Upstream kernel</a>	EoP	High	Binder driver

Android's security update summary

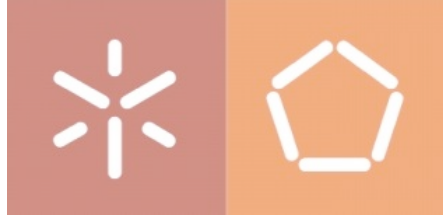
# Vulnerabilities



- 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](https://cve.mitre.org)



# 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

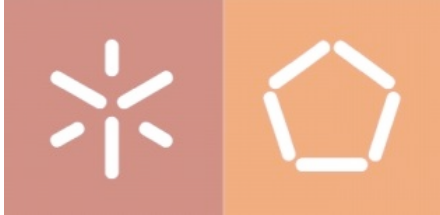
## Current Description

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:**

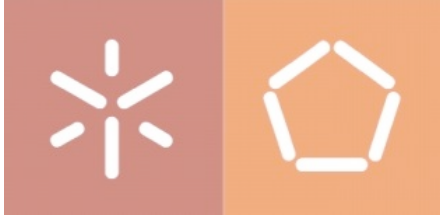
Allows unauthorized disclosure of information

Allows unauthorized modification

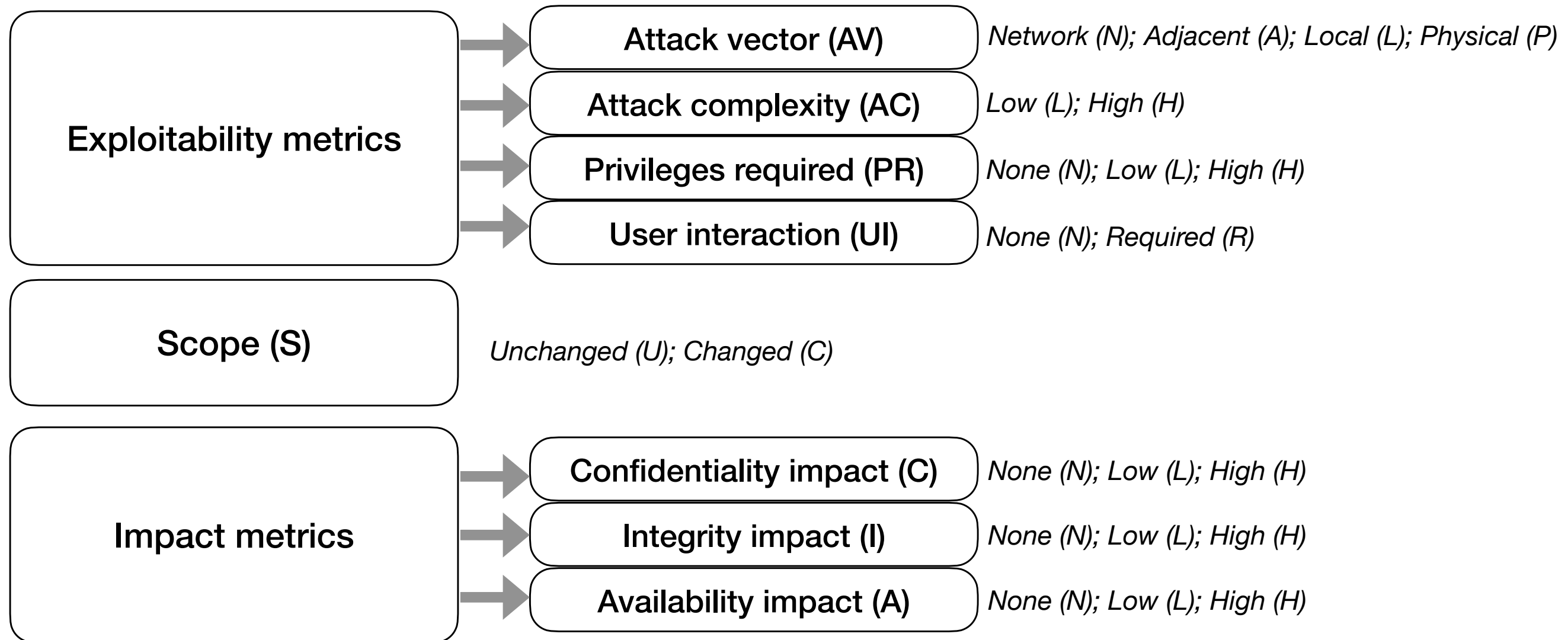
Allows disruption of service

CVSS - Common Vulnerability Scoring System

# Vulnerabilities

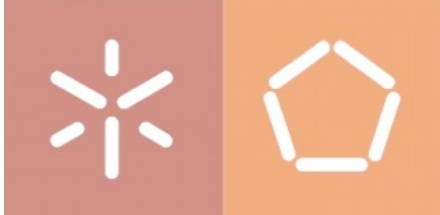


- CVSS v3.1 Base Metric Group



- See also Temporal Metrics & Environmental Metrics

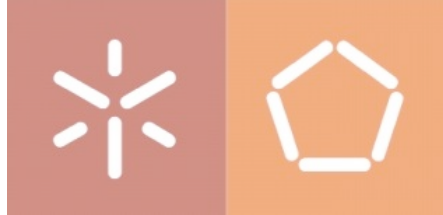
# Vulnerabilities



- CVSS v3.1: Qualitative severity rating scale

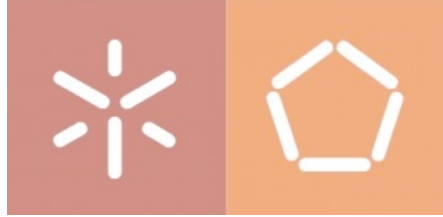
Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

# Vulnerabilities



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

# Weaknesses

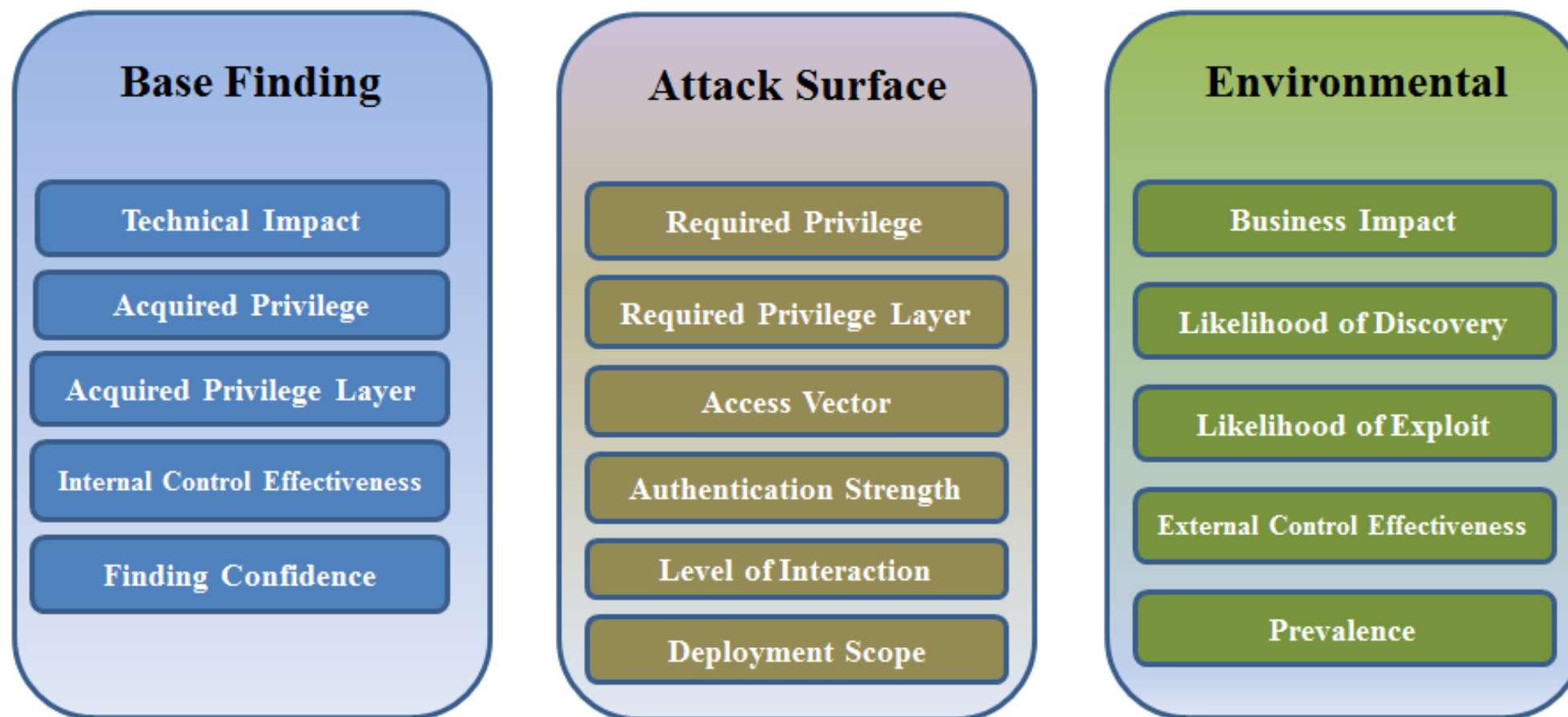


- **CWE - Common Weakness Enumeration**
  - Community-developed list of software and hardware weakness types
    - Category system
  - A baseline for weakness identification, mitigation and prevention
  - CWE List v4.2 <https://cwe.mitre.org/data/>

# Weaknesses



- **CWE - Common Weakness Enumeration**
- CWSS - Common Weakness Scoring System



Source: [cwe.mitre.org/cwss/cwss\\_v1.0.1.html](https://cwe.mitre.org/cwss/cwss_v1.0.1.html)

# 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.

## 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)

### QUICK INFO

---

**CVE Dictionary Entry:**

[CVE-2016-2107](#)

**NVD Published Date:**

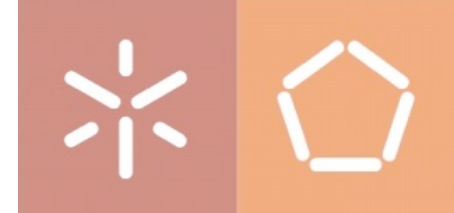
05/04/2016

**NVD Last Modified:**

07/18/2018



# Exploits



- Exploit Database - Exploit-DB
- [www.exploit-db.com](http://www.exploit-db.com)

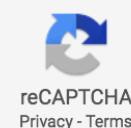
[Home](#)[Exploits](#)[Shellcode](#)[Papers](#)[Google Hacking Database](#)[Submit](#)[Search](#)

## Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

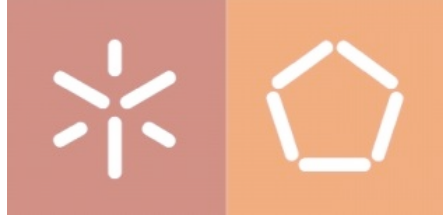


I'm not a robot

[SEARCH](#)[More Options](#)

1 total entries

Date ▾	D	A	V	Title	Platform	Author
2016-05-04	↓	-	✓	<a href="#">OpenSSL - Padding Oracle in AES-NI CBC MAC Check</a>	Multiple	Juraj...



## OpenSSL - Padding Oracle in AES-NI CBC MAC Check

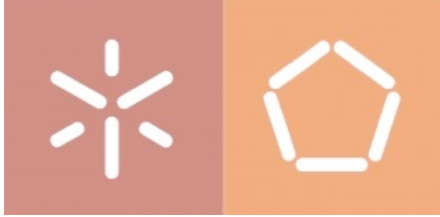
<b>EDB-ID:</b> 39768	<b>Author:</b> <a href="#">Juraj Somorovsky</a>	<b>Published:</b> 2016-05-04
<b>CVE:</b> <a href="#">CVE-2016-2107</a>	<b>Type:</b> <a href="#">Dos</a>	<b>Platform:</b> <a href="#">Multiple</a>
<b>Aliases:</b> N/A	<b>Advisory/Source:</b> <a href="#">Link</a>	<b>Tags:</b> N/A
<b>E-DB Verified:</b>	<b>Exploit:</b> <a href="#">Download</a> / <a href="#">View Raw</a>	<b>Vulnerable App:</b> N/A

[« Previous Exploit](#)

[Next Exploit »](#)

```
1 Source: http://web-in-security.blogspot.ca/2016/05/curious-padding-oracle-in-openssl-cve.html
2
3 TLS-Attacker:
4 https://github.com/RUB-NDS/TLS-Attacker
5 https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/39768.zip
6
7
8 You can use TLS-Attacker to build a proof of concept and test your implementation. You just start TLS-Attacker as follows:
9 java -jar TLS-Attacker-1.0.jar client -workflow_input rsa-overflow.xml -connect $host:$port
10
11 The xml configuration file (rsa-overflow.xml) looks then as follows:
```

# Hands-on



- Ficha de exercícios 1