Universidade do Minho
Departamento de Informática

Security Technologies

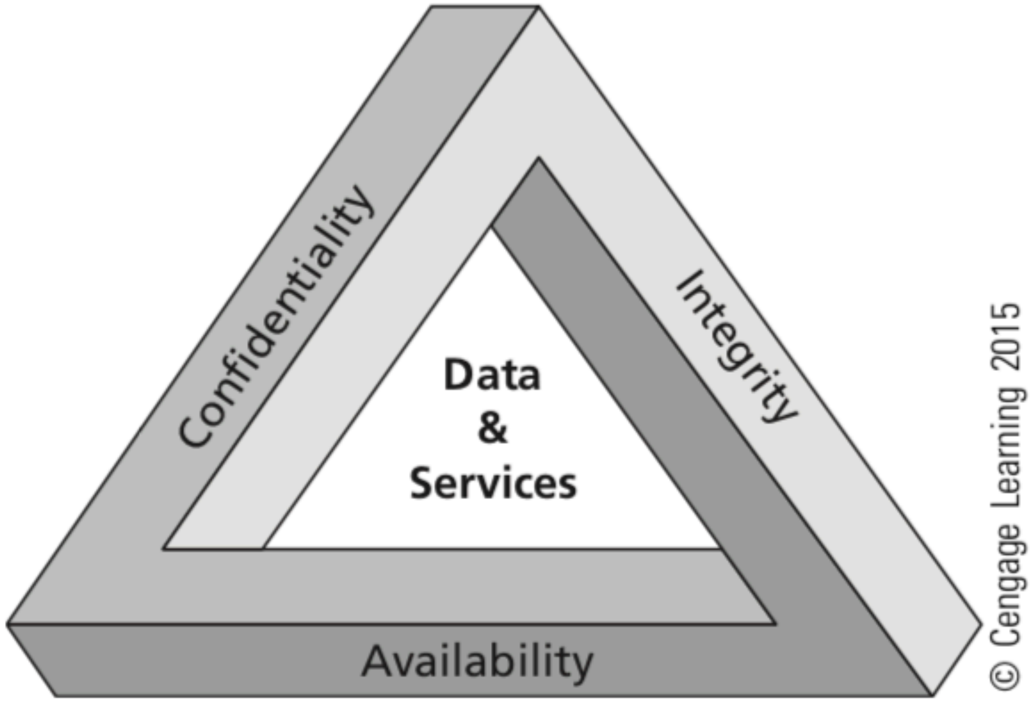
João Marco Silva
joaomarco@di.uminho.pt

Registo de presença

Concepts

What is information security?

The protection of information/data and its critical elements, including the systems and hardware used to process, store, and transmit the information*.



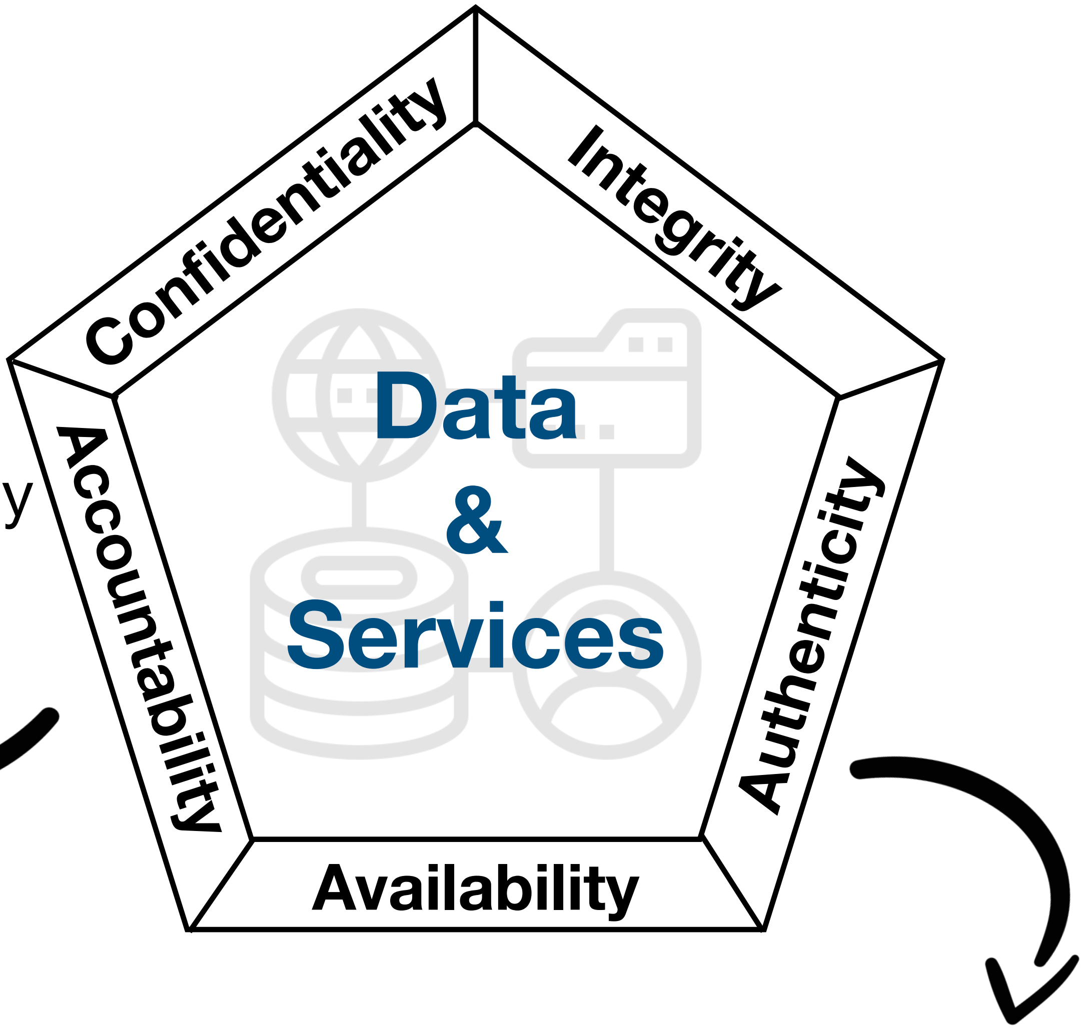
The C.I.A. triangle

* 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 consistency of information
    - involves maintaining accuracy, completeness, and trustworthiness of data over its entire life cycle
- **Availability**
  - ensures authorised users/systems to access information without interference or obstruction

Concepts



- **Non-repudiation**
  - ensures for actions of an entity to be traced uniquely to that entity

- **Authenticity**
  - ensures that data is genuine, verifiable, and trusted

Concepts

Additional key concepts

- Asset: system resources being protected
  - Hardware
  - Software
  - Data
  - Communication lines & Networks

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

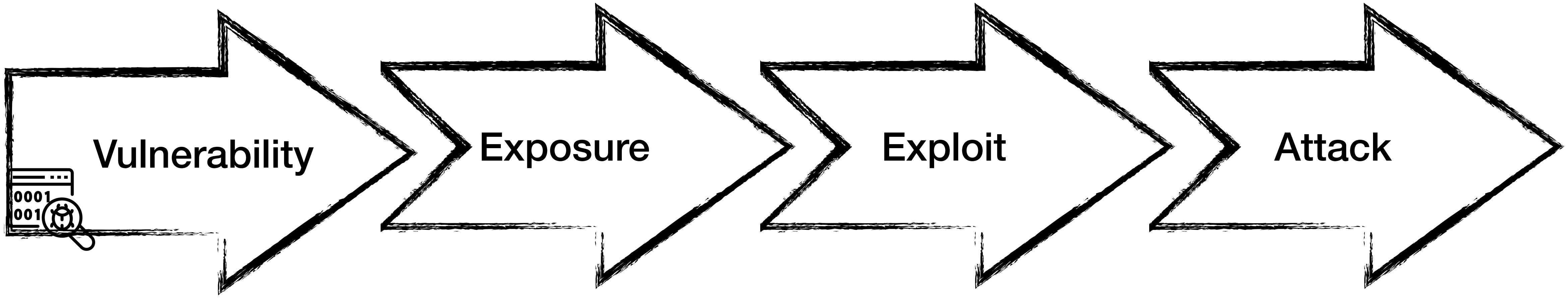
Concepts

Additional key concepts

- Attack: an intentional act that can damage or otherwise compromise information or the supporting systems
- 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



Vulnerability

Exposure

Exploit

Attack

Concepts

Additional key concepts

Assets and Example of threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service	An unencrypted USB drive is stolen	Tampering with components to gain access to I/O
Software	Programs are deleted, denying access to users	An unauthorized copy of software is produced	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task
Data	Files are deleted, denying access to users	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data	Existing files are modified or new files are fabicated
Communication lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable	Messages are read. The traffic pattern of messages is observed	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated

Concepts

Additional key concepts

- Attack surfaces

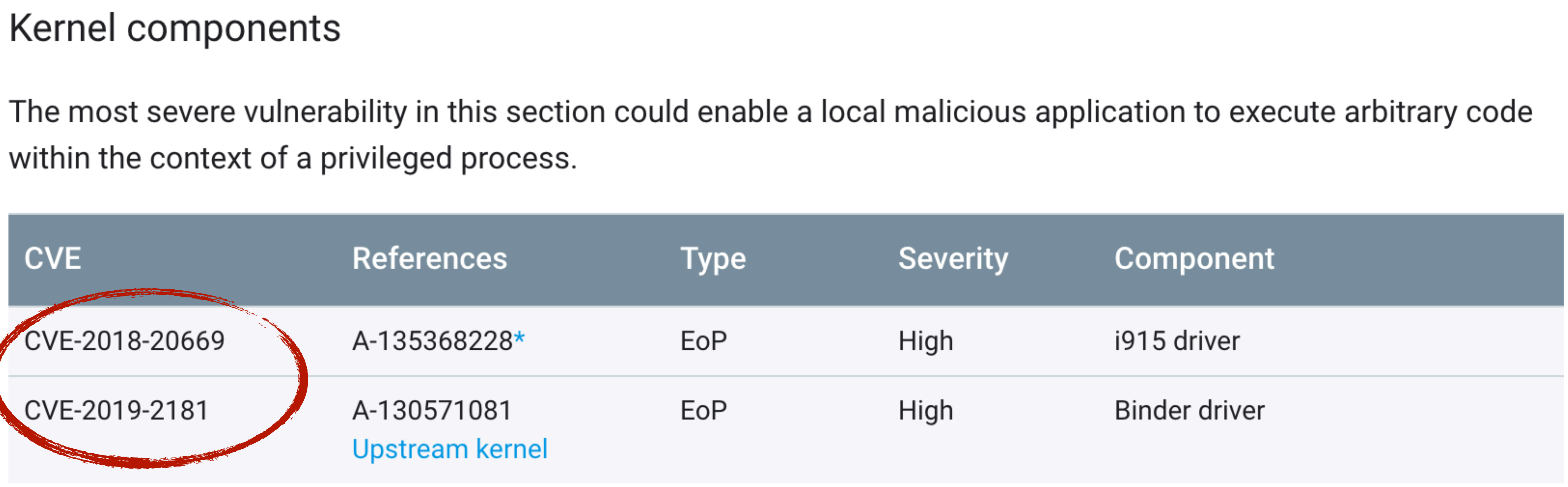
  Reachability and exploitability of system’s vulnerabilities

  - Network attack surface
  - Software attack surface
  - Human attack surface

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

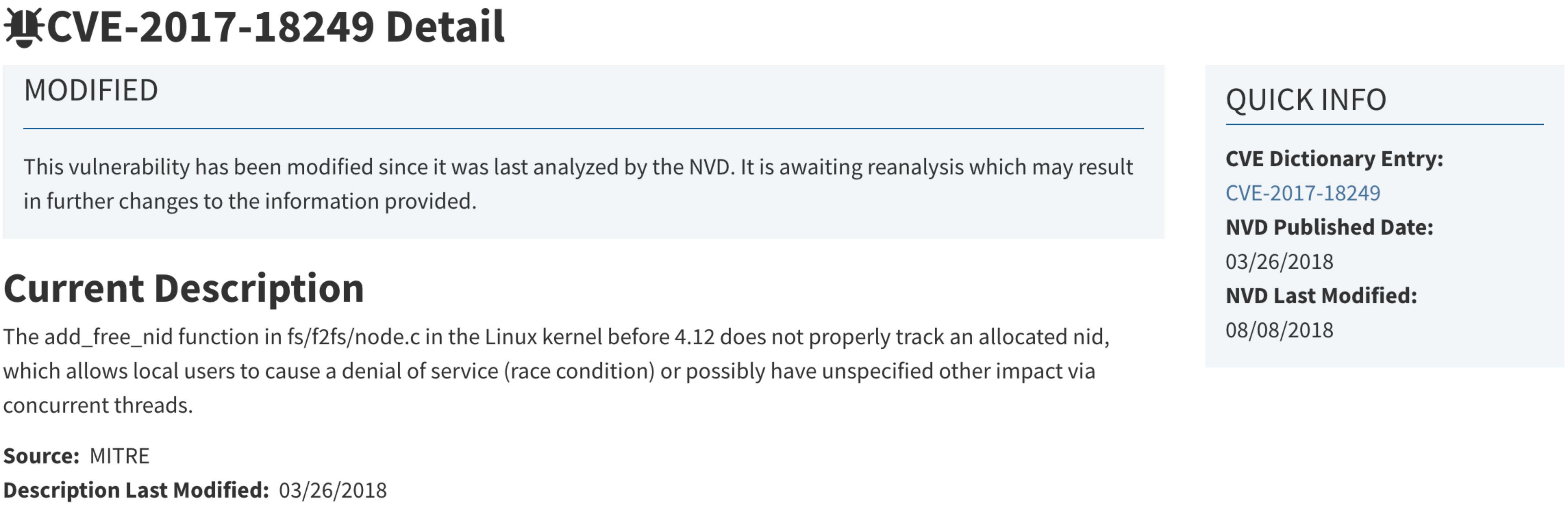
Android's security update summary

Vulnerabilities

- CVE - Common Vulnerabilities and Exposures
  - a list of standardised 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

- 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.

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.

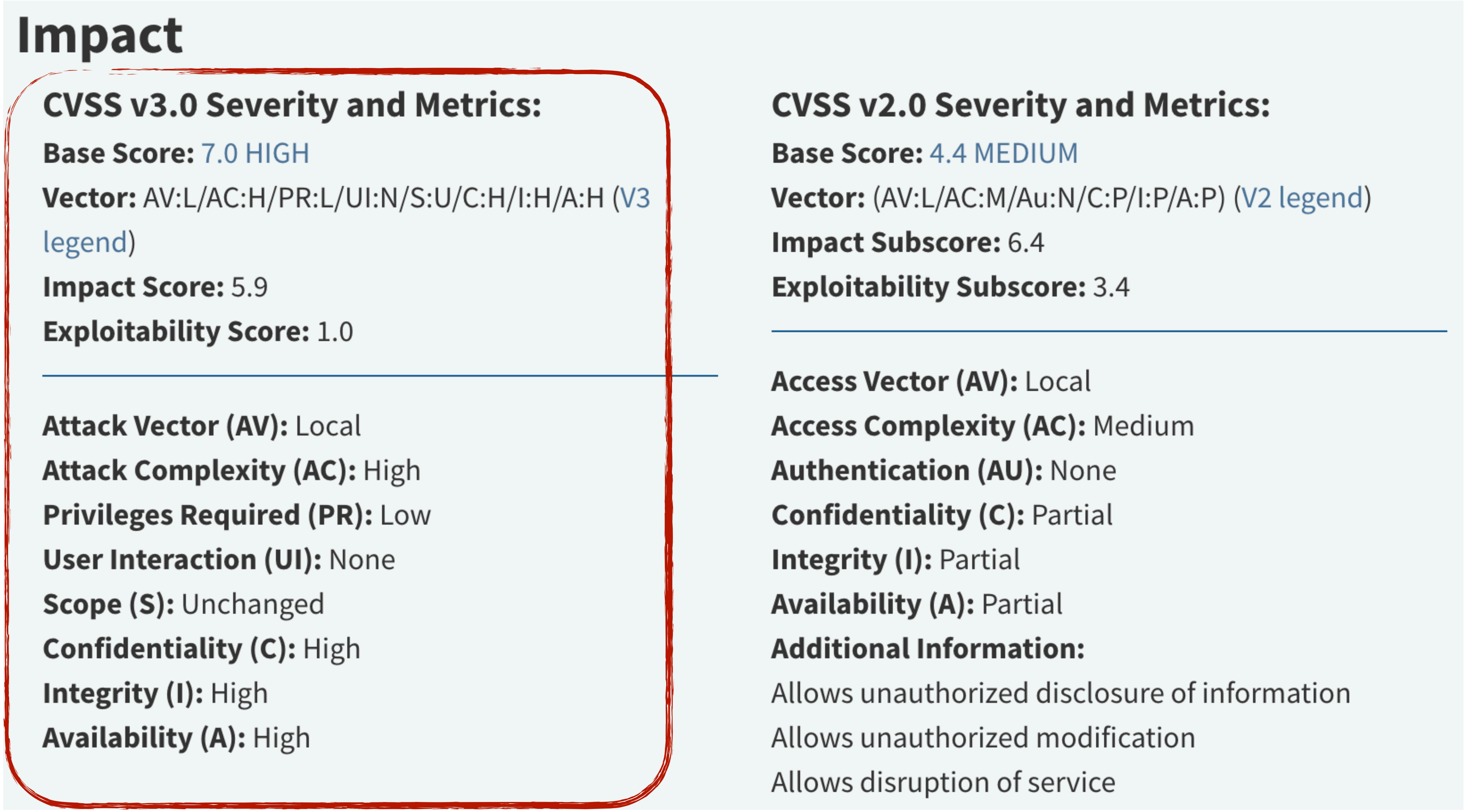
Source: MITRE
Description Last Modified: 03/26/2018

QUICK INFO

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

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

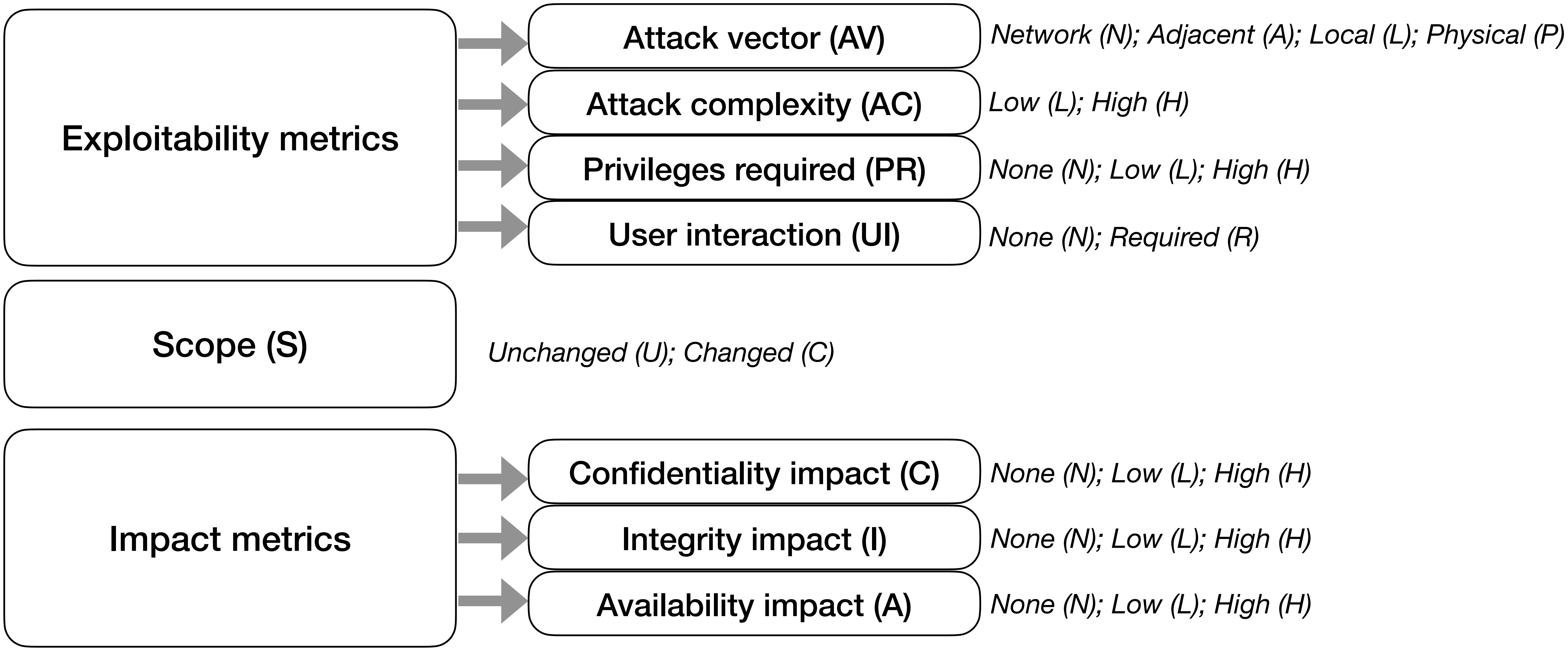
Allows unauthorized modification

Allows disruption of service

CVSS - Common Vulnerability Scoring System

Vulnerabilities

- CVSS v3.1 Base Metric Group



Exploitability metrics

Attack vector (AV) — *Network (N); Adjacent (A); Local (L); Physical (P)*

Attack complexity (AC) — *Low (L); High (H)*

Privileges required (PR) — *None (N); Low (L); High (H)*

User interaction (UI) — *None (N); Required (R)*

Scope (S) — *Unchanged (U); Changed (C)*

Impact metrics

Confidentiality impact (C) — *None (N); Low (L); High (H)*

Integrity impact (I) — *None (N); Low (L); High (H)*

Availability impact (A) — *None (N); Low (L); High (H)*

- See also Temporal Metrics & Environmental Metrics

Vulnerabilities

- CVSS v3.1: Qualitative severity rating scale

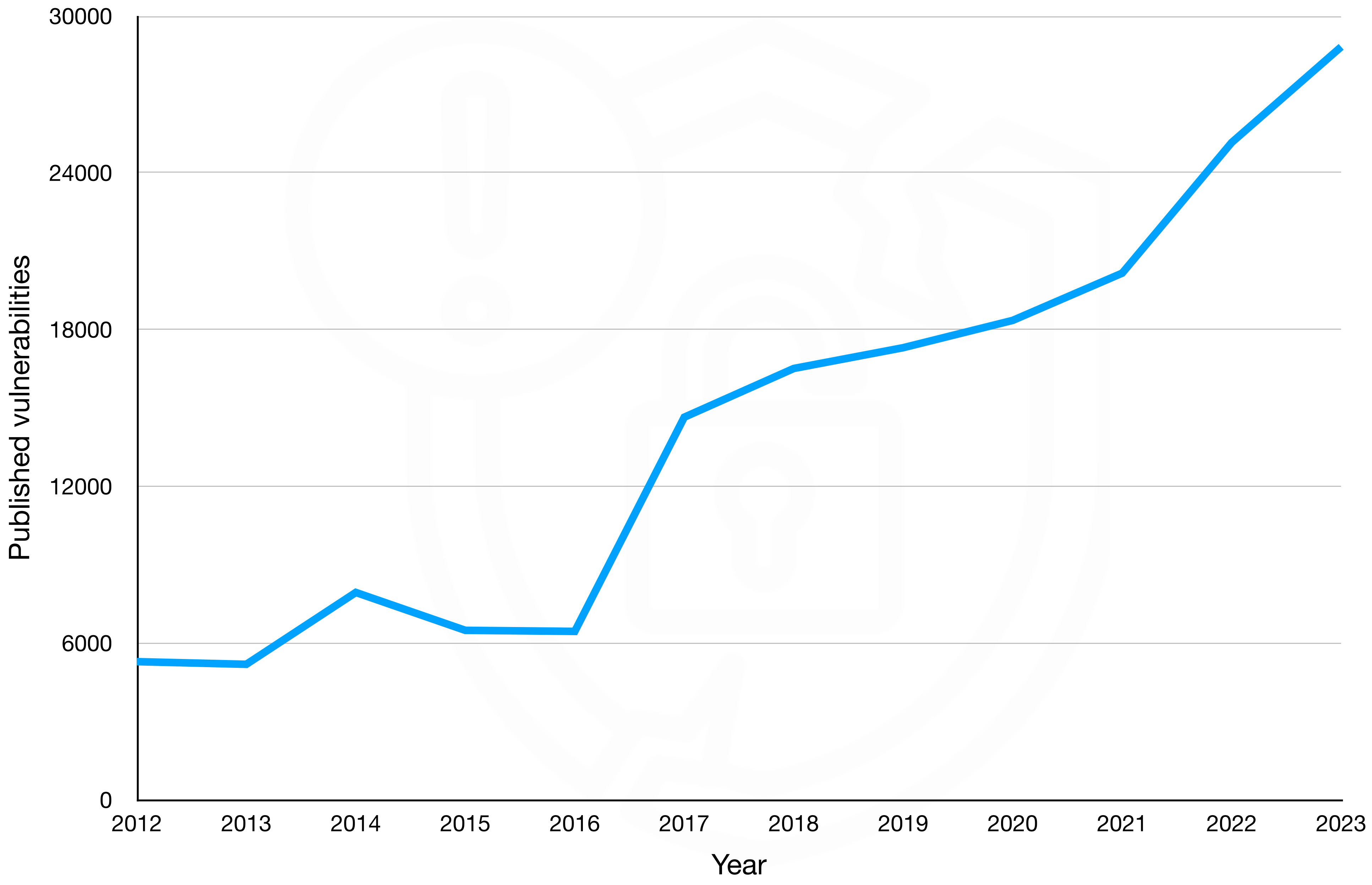
Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Vulnerabilities

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

Vulnerabilities

Landscape



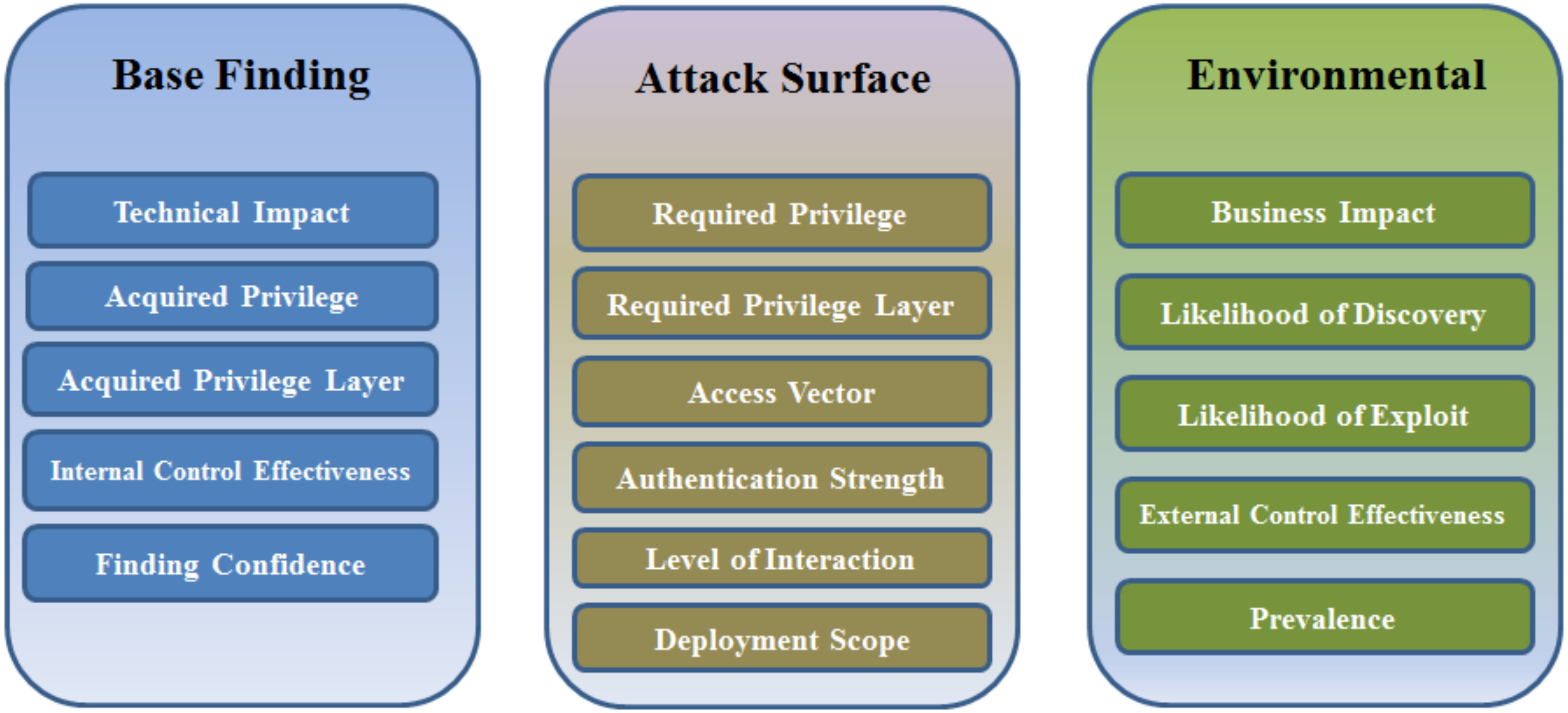
Source: NIST, 2024

Weaknesses

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

Weaknesses

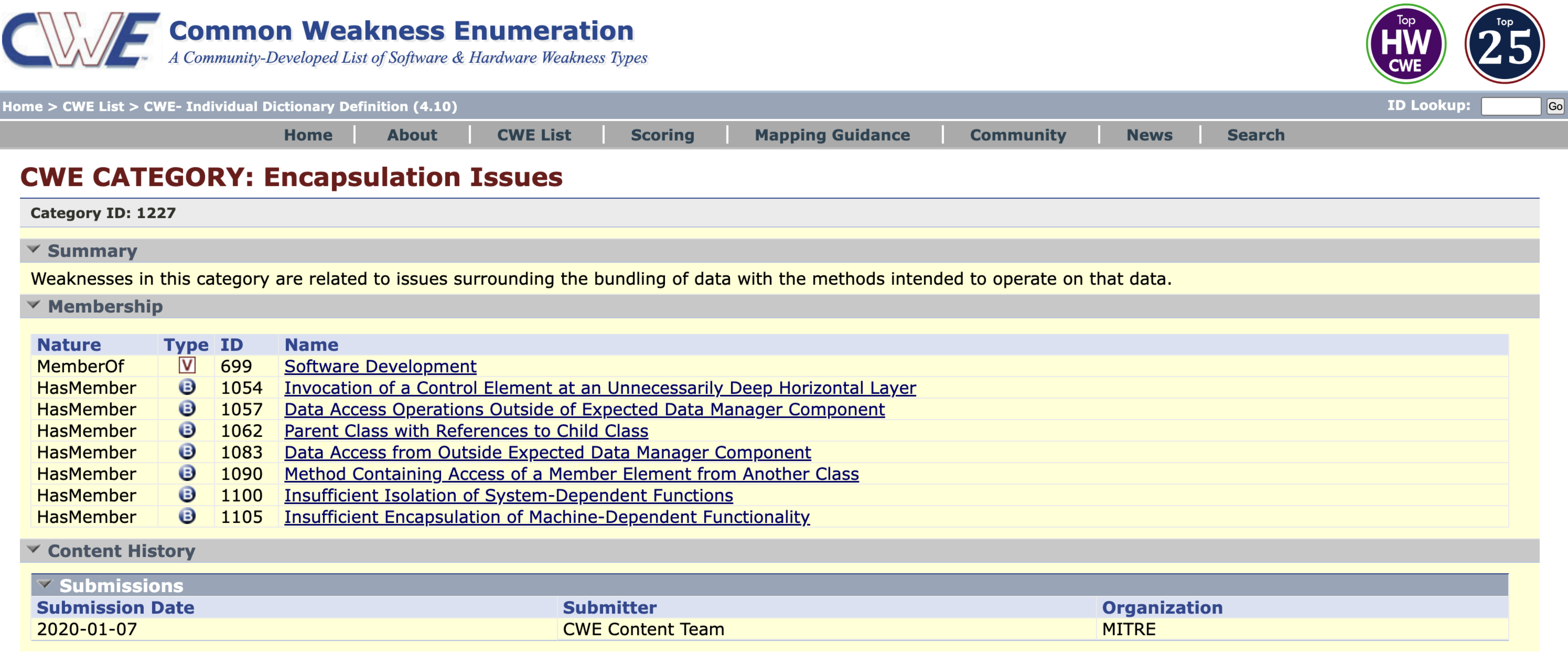
- **CWE - Common Weakness Enumeration**
  - CWSS - Common Weakness Scoring System



Source: cwe.mitre.org/cwss/cwss_v1.0.1.html

Weaknesses

- **CWE - Common Weakness Enumeration**



CWE
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
Top HW CWE
Top 25
Home > CWE List > CWE- Individual Dictionary Definition (4.10)
ID Lookup:
Go
Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

CWE CATEGORY: Encapsulation Issues

Category ID: 1227

Summary

Weaknesses in this category are related to issues surrounding the bundling of data with the methods intended to operate on that data.

Membership

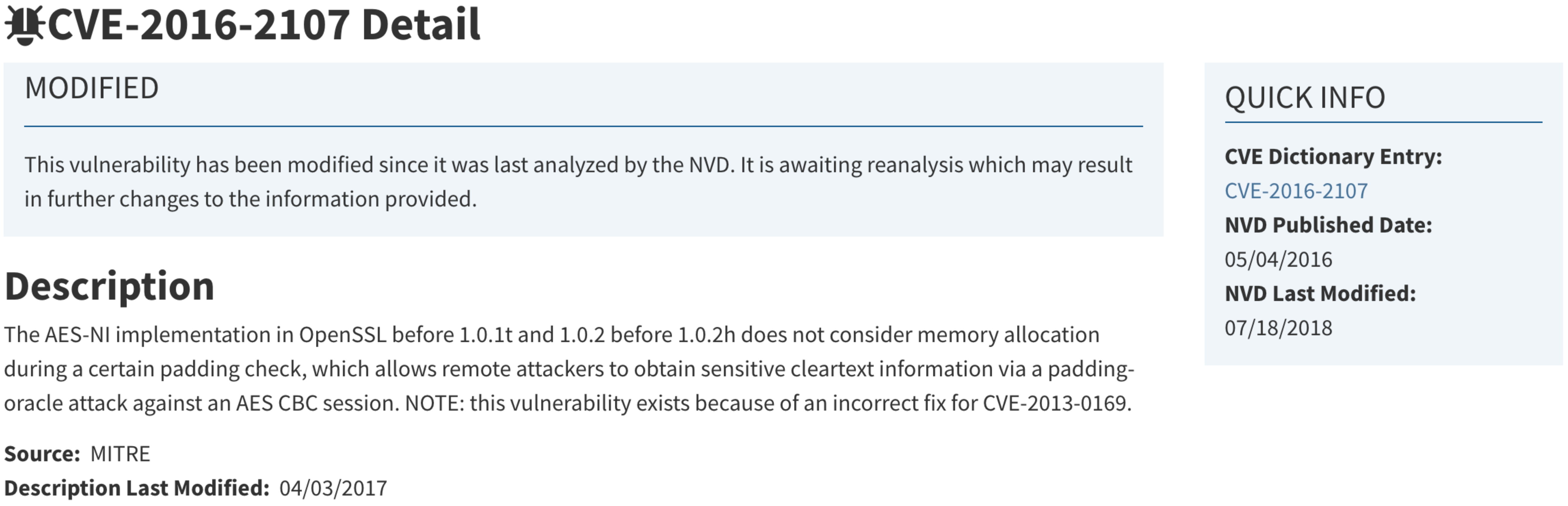
Nature	Type	ID	Name
MemberOf	V	699	Software Development
HasMember	B	1054	Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer
HasMember	B	1057	Data Access Operations Outside of Expected Data Manager Component
HasMember	B	1062	Parent Class with References to Child Class
HasMember	B	1083	Data Access from Outside Expected Data Manager Component
HasMember	B	1090	Method Containing Access of a Member Element from Another Class
HasMember	B	1100	Insufficient Isolation of System-Dependent Functions
HasMember	B	1105	Insufficient Encapsulation of Machine-Dependent Functionality

Content History

Submissions

Submission Date	Submitter	Organization
2020-01-07	CWE Content Team	MITRE

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

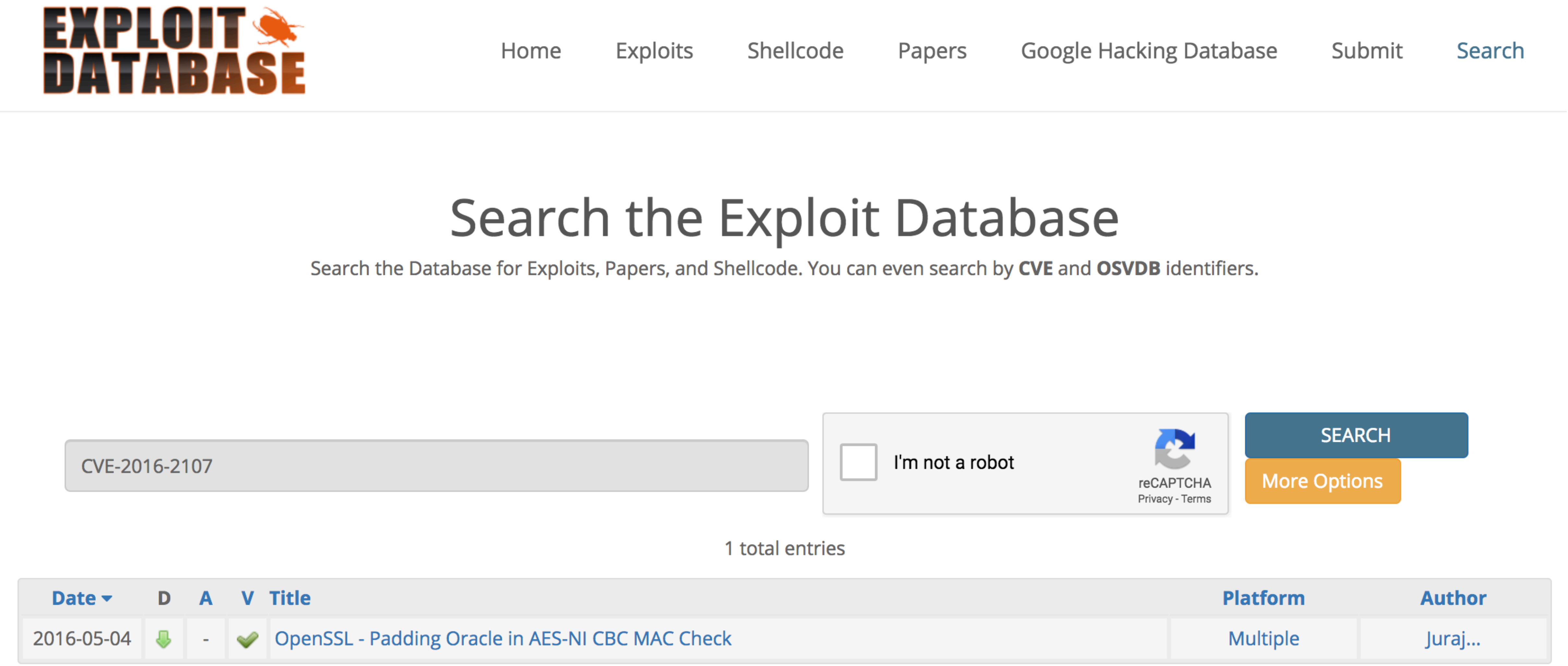
QUICK INFO

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

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

Exploits

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



Search the Exploit Database

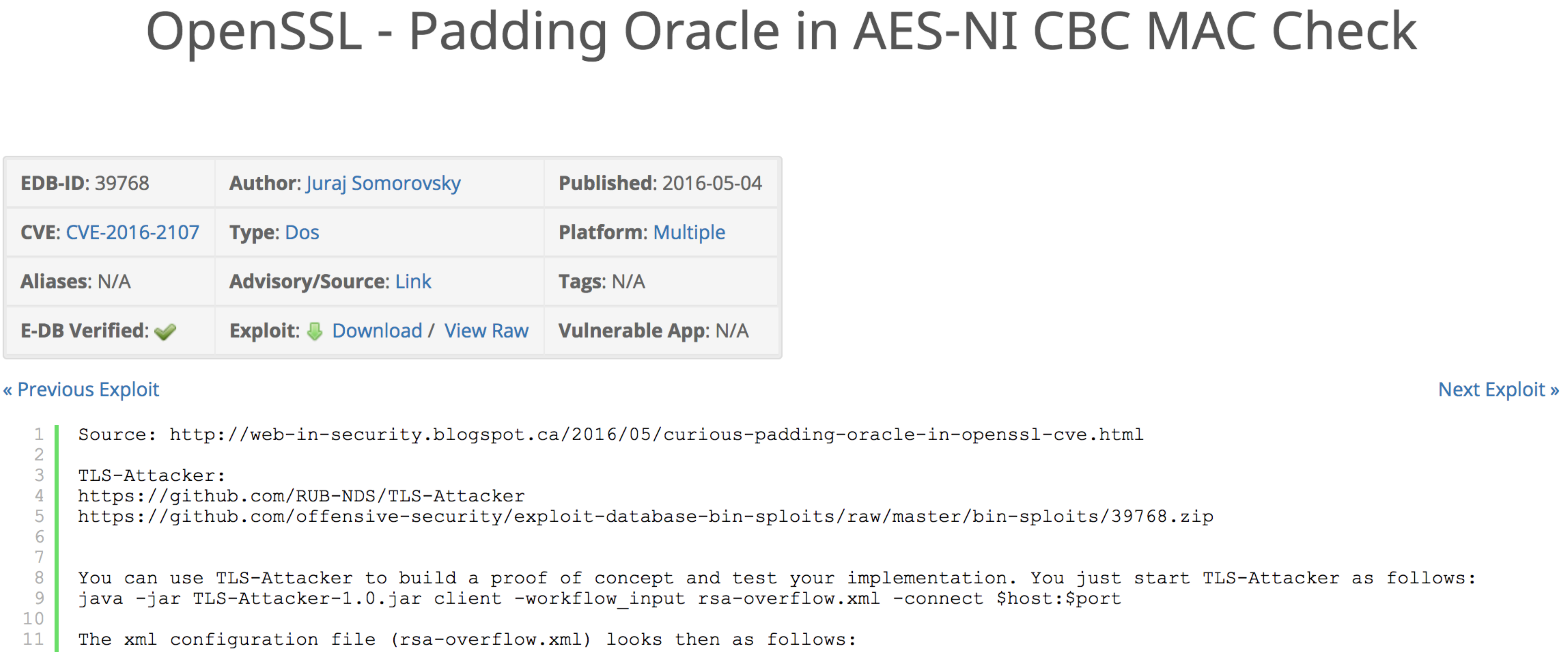
Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

CVE-2016-2107

1 total entries

Date	D	A	V	Title	Platform	Author
2016-05-04	⬇	-	✓	OpenSSL - Padding Oracle in AES-NI CBC MAC Check	Multiple	Juraj...

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:
```

Exploits

EXPLOIT DATABASE
MITRE | ATT&CK®
packet storm
0DAY.today?
OWASP®
CXSECURITY

Hands-on

- See *hands-on 1* on the e-learning platform.