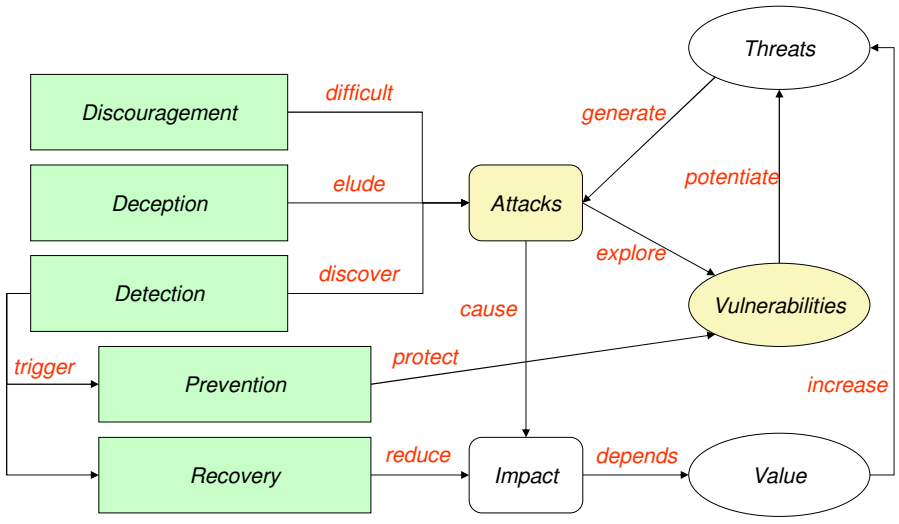
Vulnerabilities

Information Security Vulnerabilities and Attacks



Measures (and some tools)

Discouragement
- Punishment
  - Legal restrictions
  - Forensic evidences
- Security barriers
  - Firewalls
  - Autentication
  - Secure communication
  - Sandboxing

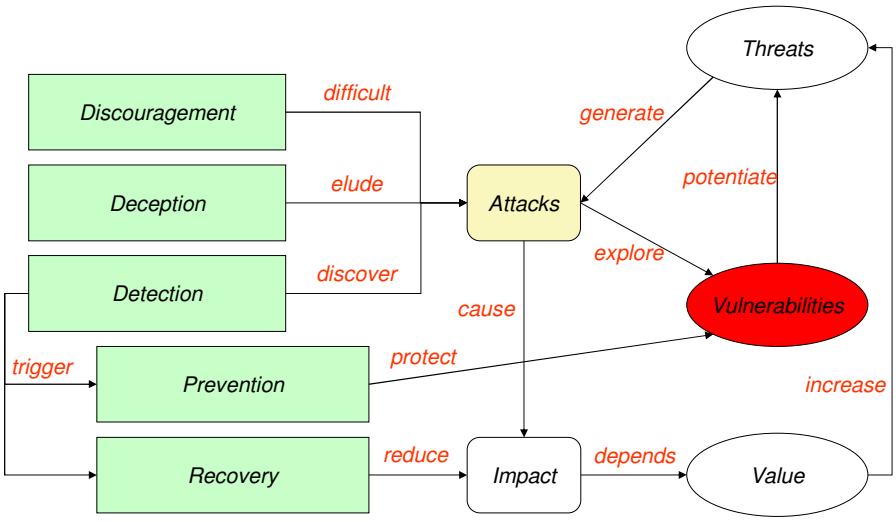
Detection
- Intrusion detection system
  - e.g. Seek, Bro, Suricata
- Auditing
- Forensic break-in analysis

Deception
- Honeypots / honeynets
- Forensic follow-up

Prevention
- Restrictive policies
  - e.g. least privilege principle
- Vulnerability scanning
  - e.g. OpenVAS, metasploit
- Vulnerability patching
  - e.g. regular updates

Recovery
- Backups
- Redundant systems
- Forensic recovery

Information Security Vulnerabilities and Attacks



Vulnerability

A mistake in software that can be directly used by an attacker to gain access to a system or network

A mistake is a vulnerability <u>if it allows an attacker to use it to violate a reasonable security policy for that system</u>

- This excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system

A CVE vulnerability is a state in a computing system (or set of systems) that either:

- Allows an attacker to execute commands as another user
- Allows an attacker to access data that is contrary to the specified access restrictions for that data
- Allows an attacker to pose as another entity
- Allows an attacker to conduct a denial of service

Exposure

A configuration issue or a mistake in software allowing access to information or capabilities used as a stepping-stone into a system or network

A configuration issue or a mistake is an exposure if it does not directly allow compromise

- But could be an important component of a successful attack, and is a violation of a reasonable security policy

An exposure describes a state in a computing system (or set of systems) that is not a vulnerability, but either:

- Allows an attacker to conduct information gathering activities
- Allows an attacker to hide activities
- Includes a capability that behaves as expected, but can be easily compromised
- Is a primary point of entry that an attacker may attempt to use to gain access to the system or data
- Is considered a problem by some reasonable security policy

CVE
Common Vulnerabilities and Exposures

Dictionary of publicly known information security vulnerabilities and exposures
- For vulnerability management
- For patch management
- For vulnerability alerting
- For intrusion detection

Uses common identifiers for the same CVEs
- Enable data exchange between security products
- Provide a baseline index point for evaluating coverage of tools and services.

Details about a vulnerability can be kept private
- Part of responsible disclosure: until owner provides a fix

CVE-ID

CVE-2015-1538 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication, aka internal bug 20139950, a related issue to CVE-2015-4496.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:76052
- URL:http://www.securityfocus.com/bid/76052
- CONFIRM:http://www.huawei.com/en/psirt/security-advisories/hw-448928
- CONFIRM:http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm
- CONFIRM:https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469f80dd9a22f1328bc81046398
- EXPLOIT-DB:38124
- URL:https://www.exploit-db.com/exploits/38124/
- MISC:http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html
- MLIST:[android-security-updates] 20150812 Nexus Security Bulletin (August 2015)
- URL:https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fi6RQM/yzJvoTVrIQAJ
- SECTRACK:1033094
- URL:http://www.securitytracker.com/id/1033094

Assigning CNA

MITRE Corporation

Date Entry Created

20150206 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20150206)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

CVE identifiers

Aka CVE names, CVE numbers, CVE-IDs, CVEs

Unique, common identifiers for publicly known information security vulnerabilities
- Have "candidate" or "entry" status
- Candidate: under review for inclusion in the list
- Entry: accepted to the CVE List

Format
- CVE identifier number (CVE-Year-Order)
- Status (Candidate or Entry)
- Brief description of the vulnerability or exposure
- References to extra information

CVE benefits

Provides common language for referring to problems
- Facilitates data sharing among
- Intrusion detection systems
- Assessment tools
- Vulnerability databases
- Researchers
- Incident response teams

Will lead to improved security tools
- More comprehensive, better comparisons, interoperable
- Indications and warning systems

Will spark further innovations
- Focal point for discussing critical database content issues

CVE and Attacks

Attacks can be made possible through multiple vulnerabilities
- One CVE for each vulnerability

Example: Stagefright (Android, video in MMS messages)
- CVE-2015-1538, P0006, Google Stagefright 'stsc' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright 'ctts' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright 'stts' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright 'stss' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1539, P0007, Google Stagefright 'esds' MP4 Atom Integer Underflow Remote Code Execution
- CVE-2015-3827, P0008, Google Stagefright 'covr' MP4 Atom Integer Underflow Remote Code Execution
- CVE-2015-3826, P0009, Google Stagefright 3GPP Metadata Buffer Overread
- CVE-2015-3828, P0010, Google Stagefright 3GPP Integer Underflow Remote Code Execution
- CVE-2015-3824, P0011, Google Stagefright 'tx3g' MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-3829, P0012, Google Stagefright 'covr' MP4 Atom Integer Overflow Remote Code Execution

Vulnerability detection

Specific tools can detect vulnerabilities
- Exploiting known vulnerabilities
- Testing known vulnerability patterns
  - e.g., buffer overflow, SQL injection, XSS, etc.

Specific tools can replicate known attacks
- Use known exploits for known vulnerabilities
  - e.g.: MS Samba v1 exploit used by WannaCry
- Can be used to implement countermeasures

Vital to assert the robustness of production systems and applications
- Service often provided by third-party companies

Vulnerability detection

Can be applied to:

- Source code (static analysis)
  - OWASP LAPSE+, RIPS, Veracode, …
- Running application (dynamic analysis)
  - Valgrind, Rational, AppScan, GCC, …
- Externally as a remote client:
  - OpenVAS, Metasploit, …

Should not be <u>blindly</u> applied to production systems!

- Potential data loss/corruption
- Potential DoS
- Potential illegal activity

CWE
Common Weakness Enumeration

Common language of discourse for discussing, finding and dealing with the causes of software security vulnerabilities

- Found in code, design, or system architecture
- Each individual CWE represents a single vulnerability type
- Currently maintained by the MITRE Corporation
  - A detailed CWE list is currently available at the MITRE website
- The list provides a detailed definition for each individual CWE

Individual CWEs are held within a hierarchical structure

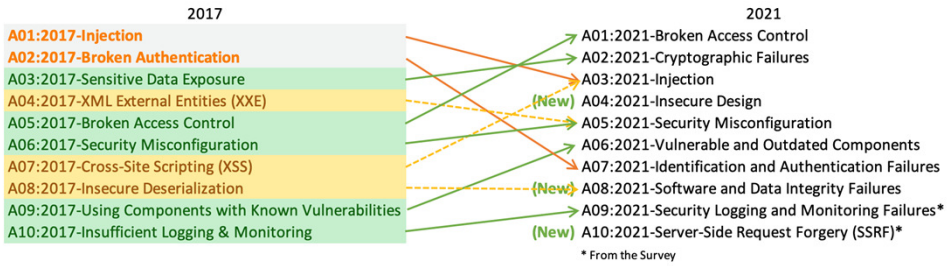
- CWEs at higher levels provide a broad overview of a vulnerability type
  - Can have many children CWEs associated with them
- CWEs at deeper levels provide a finer granularity
  - Usually have fewer or no children CWEs

CWE ≠ CVE

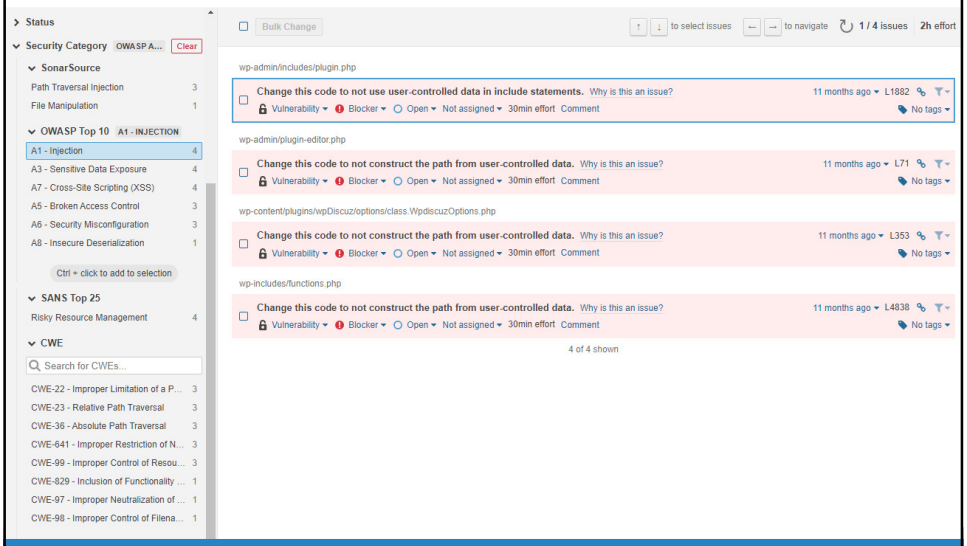
Vulnerability types
OWASP Top 10 (Web, 2021)

1. Broken Access control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

Vulnerability types
OWASP Top 10 (Web)



Static Analysis (with Sonarcloud)



Vulnerability Tracking by vendors

During the development cycle, vulnerabilities are handled as bugs

- May have a dedicated security team or not

When software is available, vulnerabilities are also tracked globally

- For every system and software publicly available

Public tracking helps…

- focusing the discussion around the same issue
  - Ex: a library that is used in multiple applications, distributions
- defenders to easily test their systems, enhancing the security
- attackers to easily know what vulnerability can be used

Vulnerability Tracking

Vulnerabilities are privately tracked

- Constitute an arsenal for future attacks against targets
- Exploits are weapons

Knowledge about vulnerabilities and exploits is publicly traded

- From 0 to 2-3M€ (more?) through direct markets, or acquisition programs
- Up to 2.5M€ for bug hunting programs or direct acquisition (Google, Zerodium)
  - 2.5M€: 1 click Android exploit
  - 2M€: 1 click iPhone exploit
  - 1.5M€: WhatsApp or iMessage exploit
  - ~2K for a XSS at HackerOne (although there are records of $1M payouts)

…and privately traded at unknown prices

- Private Companies, Organized Crime, APTs

CVE-2020-1472

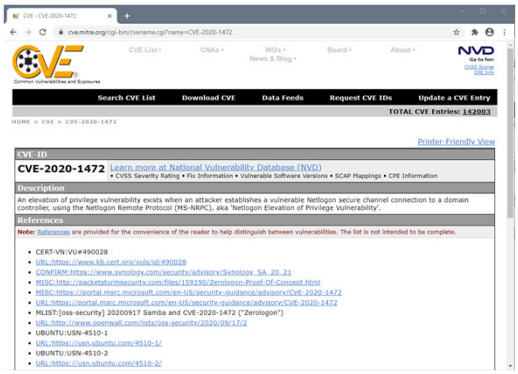
@MITRE

Basic information about the CVE

References to other trackers (provided for convenience)

Vendor pages

Mailing lists



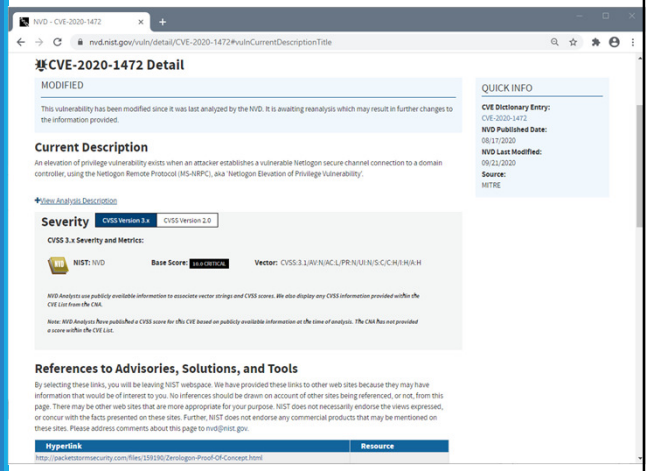
CVE-2020-1472

@NVD

Basic information about the CVE and a small analysis of it

The CVE Severity Score

Links to advisories, solutions



CVE-2020-1472

@Product Owner

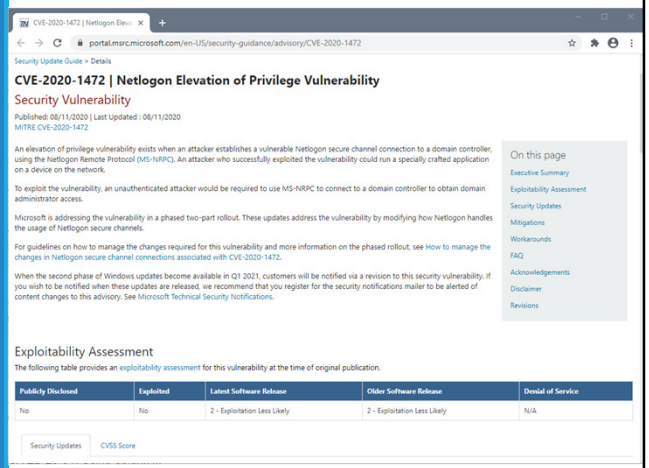
More detail, why it happens, and how it can be mitigated

Information about patches/updates available to help IT staff and users

Information about it's exploitability

Format is vendor dependent

Each vendor defines what/how to show information



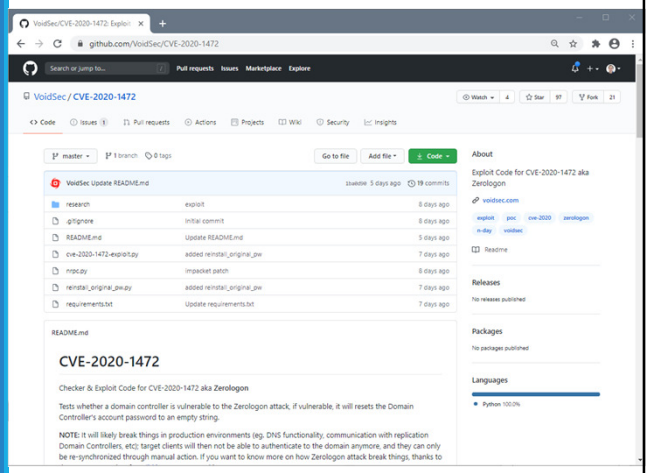
CVE-2020-1472

@Other places

Independent researchers may publish Proofs of concept (PoC)

Very dynamic community with public and private facets

PoC may help both defenders and attackers
- **Defenders can test**
- **Attackers have code to use**

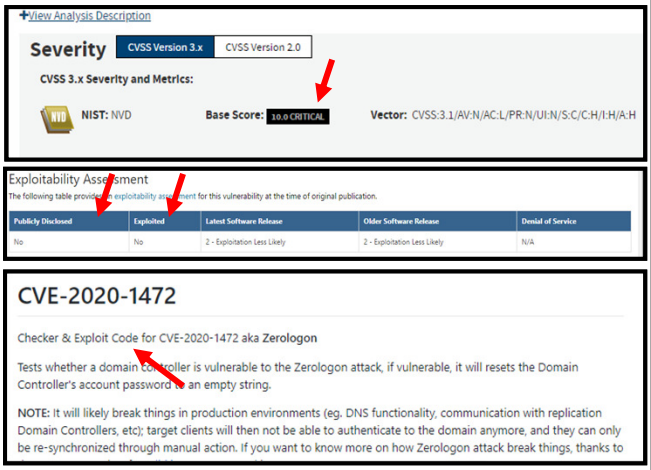


Vulnerability tracking

Not an easy task
- Exploits are not always known
- Impact and Value may be underestimated

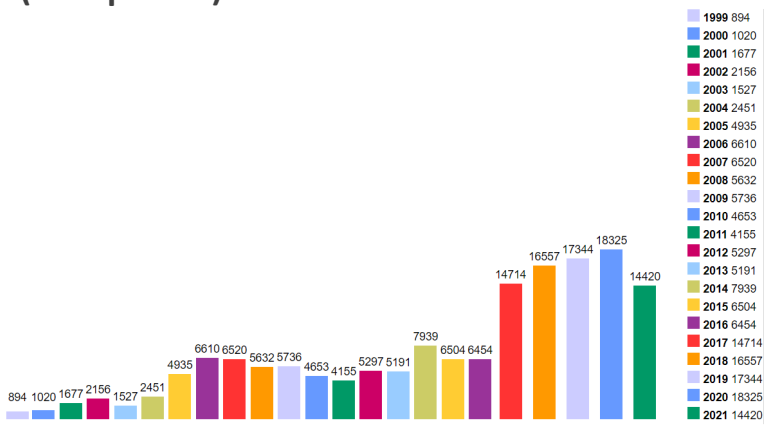
Old feeds may create a false sense of security

A highly dynamic community is great…
- To defenders as they can test and implement defenses
- To attackers as they can incorporate exploits



CVE per year – cvedetails.com

(at Sep 2021)



Zero Day (or Zero Hour) Attack/Threat

Attack using vulnerabilities which are:

- Unknown to others
- Undisclosed to the software vendor

Occurs at the day zero of the knowledge about those vulnerabilities

- For which no security fix is available

A single "day zero" may exist for months/years

- Known to attackers, unknown to others
- Frequently part of attack arsenal
- Traded around in specific markets

Survivability

How can we survive a zero-day attack?

How can we react to a massive zero-day attack?

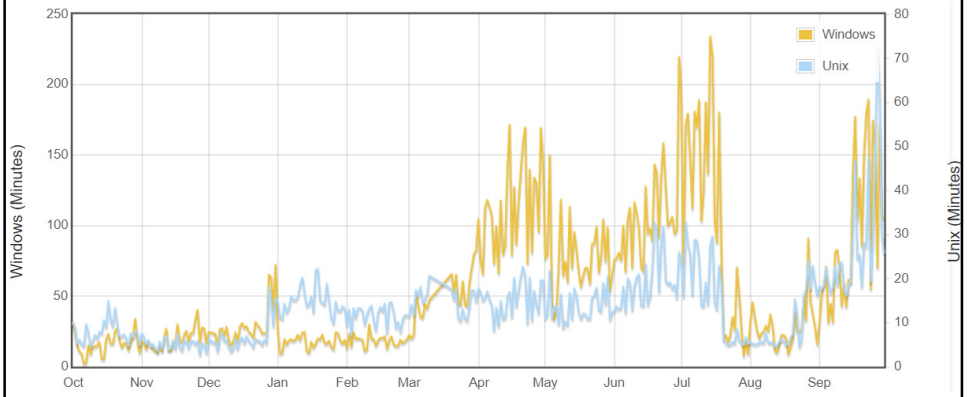
Diversity is one answer (as a policy) …

- but software production, distribution and update goes on the opposite direction!
  - And the same happens with hardware architectures
- Why is MS Windows such an interesting target?
  - And Apple macOS not so much?
- Are you using an Android cell phone?
  - What are the odds of being in the battlefront? (you are)
  - iOS landscape may be worst as it is more homogeneous

Mean Survival Time

Oct 2020 – Oct 2021

(http://isc.sans.org/survivaltime.html)



Defender will constantly spend resources in security

Attacker only needs to be successful once

- Attackers can screen for victims with low effort and in an automated manner

CERT
Computer Emergency Readiness Team

Organization ensuring that appropriate technology and systems' management practices are used to

- Resist attacks on networked systems
- Limit damage, ensure continuity of critical services
  - In spite of successful attacks, accidents, or failures

CERT/CC (Coordination Center) @ CMU

- One component of the larger CERT Program
- A major center for internet security problems
  - Established in November 1988, after the "Morris Worm"
  - It demonstrated the growing Internet exposure to attacks

CSIRT
Computer Security Incident Response Team

A service organization responsible for receiving, reviewing, and responding to computer security incident reports and activity

- Provides 24x7 Computer Security Incident Response Services to users, companies, government agencies or organizations
- Provides a reliable and trusted single point of contact for reporting computer security incidents worldwide
- CSIRT provides the means for reporting incidents and for disseminating important incident-related information

Portuguese CSIRTs

- CERT.PT: https://www.facebook.com/CentroNacionalCibersegurancaPT
- National CSIRT Network : https://www.redecsirt.pt/
- CSIRT @ UA: https://csirt.ua.pt

Security alerts & activity trends

Vital to the fast dissemination of knowledge about new vulnerabilities

- US-CERT Technical Cyber Security Alerts
- US-CERT (non-technical) Cyber Security Alerts
- SANS Internet Storm Center
  - Aka DShield (Defense Shield)
- Microsoft Security Response Center
- Cisco Security Center

- And many others …

Other sources of information

Reddit r/netsec

Twitter #infosec #cybersec

Discord, Slack and other private and public sources

- https://en.0day.today
- https://www.exploit-db.com/
- https://vuldb.com/