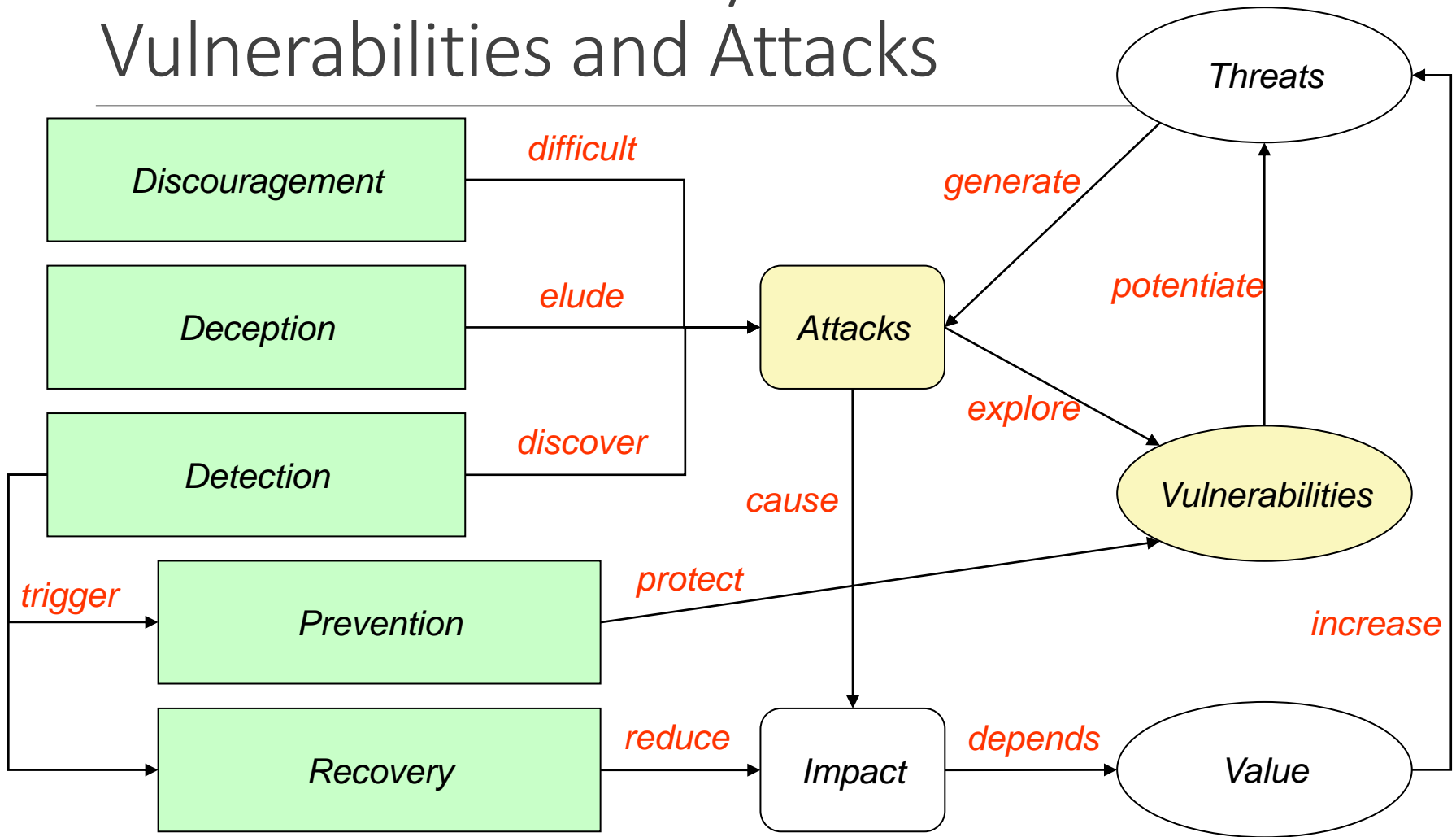


# Vulnerabilities

---

# 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

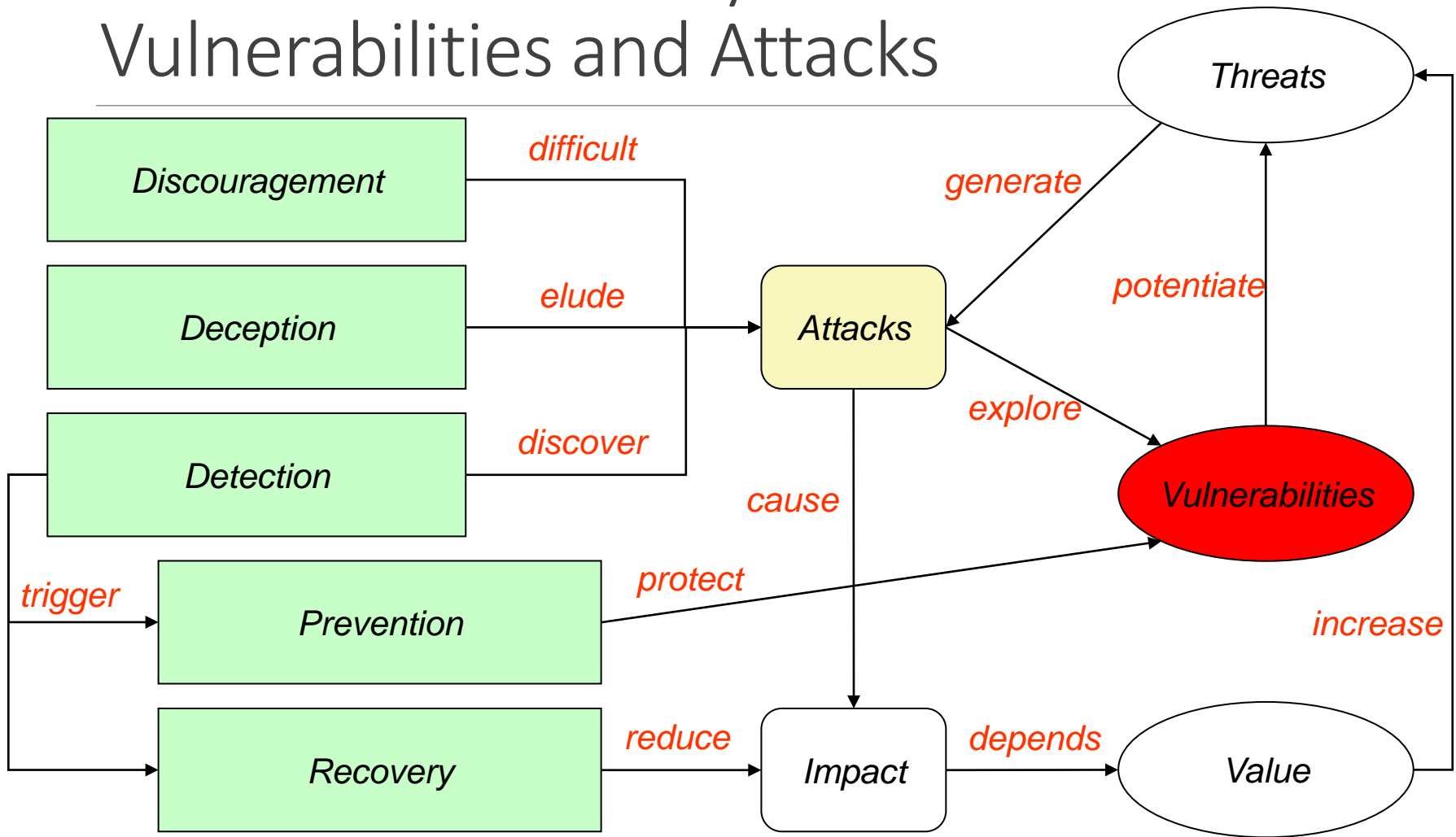
## Prevention

- 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 if it allows an attacker to use it to violate a reasonable security policy for that system**

- 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

# Security readiness (1/3)

---

## **Discouragement, Deception and Detection measures mainly tackle known issues**

- Reconnaissance attempts (e.g. port scanning)
- Generic attacks (e.g. network eavesdropping)
- Specific attacks (e.g. buffer overflows)

## **Prevention measures tackle well-known and unknown vulnerabilities**

- Generic vulnerabilities
  - e.g. reaction to malformed messages (protocol scrubbers)
  - e.g. stealth attacks (normalization to canonical formats)
- Specific vulnerabilities (e.g. a particular software bug)

# Security readiness (2/3)

---

## Measure enforcement requires specific knowledge

### Known vulnerabilities

- Problem, exploitation mode, impact, etc.

### Activity patterns used in attacks

- Modus operandi
- Attacks' signatures

### Abnormal activity patterns

- Abnormal is the opposite of normal ...
  - ...but what's normal?
- Hard to define in heterogeneous environments

source: flickr





1

DEVICE



1 Year Subscription  
Abonnement d'un an

Includes Antivirus Security  
Comprend la protection  
antivirus

**100%**

**GUARANTEE / GARANTIE  
DE PROTECTION COMPLÈTE\***

Viruses removed or your money back  
Éradication des virus garantie ou argent remis

Always updated to the latest version  
Une protection toujours dotée de la version la plus récente



Internet Connection Required  
Connexion Internet requise

# Security readiness (3/3)

---

## **Computer network threats are not like other threats**

- They can be launched anytime, anywhere
- They can be easily coordinated, and chain multiple attacks
  - e.g. Distributed Denial of Service attacks (DDoS)
- They are cheap to deploy
- They can be automated
- They are fast

## **Thus, they require a permanent, 24x7 capacity to react to attacks:**

- Teams of security experts
- Just-in-time attack alerts
- Security measurement and evaluation
- Immediate reaction procedures

# 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 CVE's**

- 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	
<b>CVE-2015-1538</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • 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	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"> <li>BID:76052</li> <li>URL:<a href="http://www.securityfocus.com/bid/76052">http://www.securityfocus.com/bid/76052</a></li> <li>CONFIRM:<a href="http://www.huawei.com/en/psirt/security-advisories/hw-448928">http://www.huawei.com/en/psirt/security-advisories/hw-448928</a></li> <li>CONFIRM:<a href="http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm">http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm</a></li> <li>CONFIRM:<a href="https://android.googlesource.com/platform/frameworks/av/+2434839bbd168469f80dd9a22f1328bc81046398">https://android.googlesource.com/platform/frameworks/av/+2434839bbd168469f80dd9a22f1328bc81046398</a></li> <li>EXPLOIT-DB:38124</li> <li>URL:<a href="https://www.exploit-db.com/exploits/38124/">https://www.exploit-db.com/exploits/38124/</a></li> <li>MISC:<a href="http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html">http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html</a></li> <li>MLIST:[android-security-updates] 20150812 Nexus Security Bulletin (August 2015)</li> <li>URL:<a href="https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fi6RQM/yzJvoTVrIQAJ">https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fi6RQM/yzJvoTVrIQAJ</a></li> <li>SECTrack:1033094</li> <li>URL:<a href="http://www.securitytracker.com/id/1033094">http://www.securitytracker.com/id/1033094</a></li> </ul>	
Assigning CNA	
MITRE Corporation	
Date Entry Created	
<b>20150206</b>	Disclaimer: The <a href="#">entry creation date</a> 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 <a href="#">CVE List</a> , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
<b>SEARCH CVE USING KEYWORDS:</b> <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the <a href="#">CVE Reference Maps</a> .	
<b>For More Information:</b> <a href="#">CVE Request Web Form</a> (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 blindly 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 located at higher levels provide a broad overview of a vulnerability type
  - Can have many children CWEs associated with them
- CWEs at deeper levels in the structure provide a finer granularity
  - Usually have fewer or no children CWEs

**CWE != CVE**

# Vulnerability types

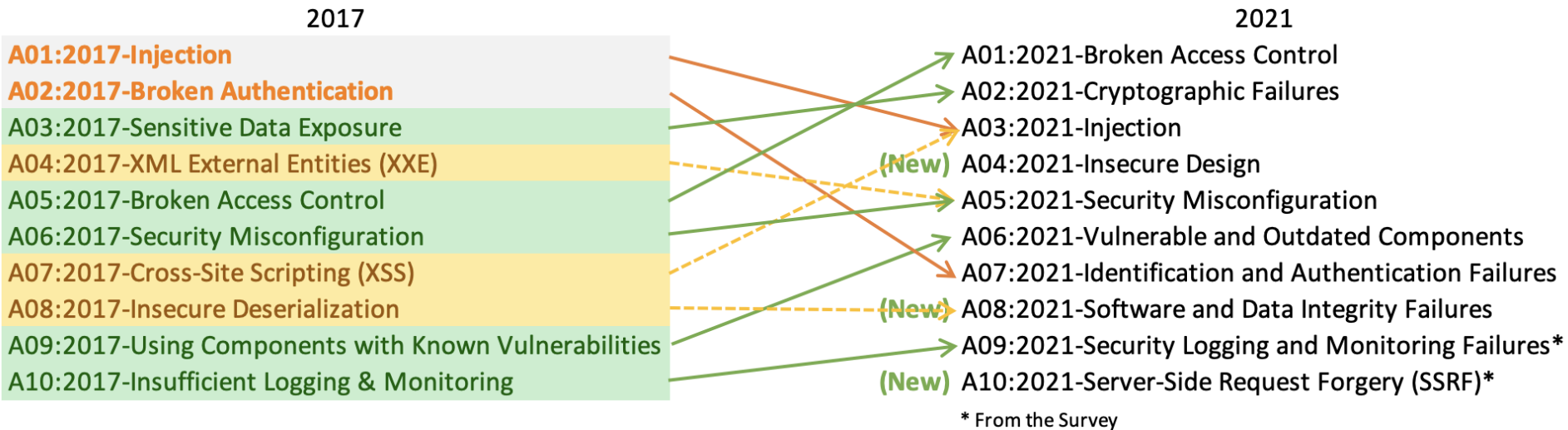
## OWASP Top 10 (Web)

---

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulns.
10. Insufficient logging and monitoring

# Vulnerability types

## OWASP Top 10 (Web)



# CWE-348: Use of Less Trusted Source

---

The software has two different sources of the same data or information, but it uses the source that has less support for verification, is less trusted, or is less resistant to attack.

Details at: <https://cwe.mitre.org/data/definitions/348.html>

- Describes pattern, provides examples, provides list of related CVEs

# CWE-348: Use of Less Trusted Source

```
$requestingIP = '0.0.0.0';
if (array_key_exists('HTTP_X_FORWARDED_FOR', $_SERVER)) {
    $requestingIP = $_SERVER['HTTP_X_FORWARDED_FOR'];
}
else{
    $requestingIP = $_SERVER['REMOTE_ADDR'];
}

if(in_array($requestingIP,$ipAllowlist)){
    generatePage();
    return;
}
else{
    echo "You are not authorized to view this page";
    return;
}
```


Set by Web  
Server  
or Client

Set by Web  
Server

# Static Analysis (with Sonarcloud)

## Reliability [Measures](#)


1.7k <sup>E</sup>

 Bugs <sup>?</sup>

started 11 months ago

## Security [Measures](#)

244 <sup>E</sup>

 Vulnerabilities <sup>?</sup>

312

 Security Hotspots <sup>?</sup>

## Maintainability [Measures](#)

271d <sup>A</sup>

Debt <sup>?</sup>

15k

 Code Smells <sup>?</sup>

## Duplications [Measures](#)



3.2%

Duplications <sup>?</sup>

2.5k

Duplicated Blocks <sup>?</sup>

# Static Analysis (with Sonarcloud)

**Status**

**Security Category** OWASP A... Clear

**SonarSource**

- Path Traversal Injection 3
- File Manipulation 1

**OWASP Top 10** **A1 - INJECTION**

- A1 - Injection 4
- A3 - Sensitive Data Exposure 4
- A7 - Cross-Site Scripting (XSS) 4
- A5 - Broken Access Control 3
- A6 - Security Misconfiguration 3
- A8 - Insecure Deserialization 1

Ctrl + click to add to selection

**SANS Top 25**

- Risky Resource Management 4

**CWE**

Search for CWEs...

- CWE-22 - Improper Limitation of a P... 3
- CWE-23 - Relative Path Traversal 3
- CWE-36 - Absolute Path Traversal 3
- CWE-641 - Improper Restriction of N... 3
- CWE-99 - Improper Control of Resou... 3
- CWE-829 - Inclusion of Functionality ... 1
- CWE-97 - Improper Neutralization of ... 1
- CWE-98 - Improper Control of Filena... 1

**Issues Summary:**

- wp-admin/includes/plugin.php**
  - ☐ **Change this code to not use user-controlled data in include statements.** [Why is this an issue?](#) 11 months ago ▾ L1882 🔗 ⚙️ ▾  
🔒 Vulnerability ▾ 🚫 Blocker ▾ 🔵 Open ▾ ⚪ Not assigned ▾ 30min effort [Comment](#) No tags ▾
- wp-admin/plugin-editor.php**
  - ☐ **Change this code to not construct the path from user-controlled data.** [Why is this an issue?](#) 11 months ago ▾ L71 🔗 ⚙️ ▾  
🔒 Vulnerability ▾ 🚫 Blocker ▾ 🔵 Open ▾ ⚪ Not assigned ▾ 30min effort [Comment](#) No tags ▾
- wp-content/plugins/wpDiscuz/options/class.WpdiscuzOptions.php**
  - ☐ **Change this code to not construct the path from user-controlled data.** [Why is this an issue?](#) 11 months ago ▾ L353 🔗 ⚙️ ▾  
🔒 Vulnerability ▾ 🚫 Blocker ▾ 🔵 Open ▾ ⚪ Not assigned ▾ 30min effort [Comment](#) No tags ▾
- wp-includes/functions.php**
  - ☐ **Change this code to not construct the path from user-controlled data.** [Why is this an issue?](#) 11 months ago ▾ L4838 🔗 ⚙️ ▾  
🔒 Vulnerability ▾ 🚫 Blocker ▾ 🔵 Open ▾ ⚪ Not assigned ▾ 30min effort [Comment](#) No tags ▾

4 of 4 shown



# 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

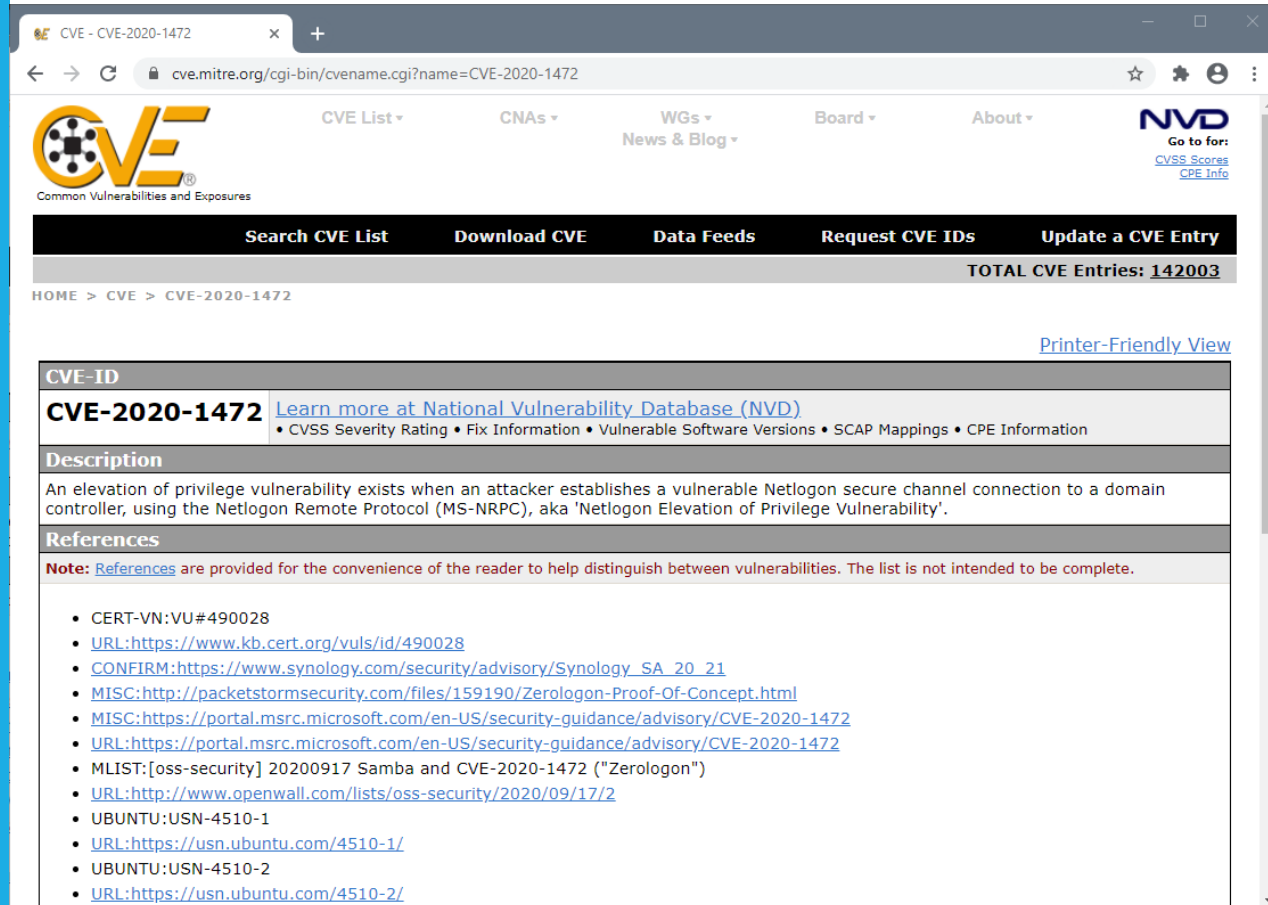
## @MITRE

Basic information  
about the CVE

References to other  
trackers (provided for  
convenience)

Vendor pages

Mailing lists



The screenshot shows the MITRE CVE website page for CVE-2020-1472. The browser address bar shows the URL `cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472`. The page features the MITRE logo and navigation links for CVE List, CNAs, WGs, Board, and About. A secondary navigation bar includes links for Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. The total number of CVE entries is displayed as 142003. The main content area for CVE-2020-1472 includes a description of an elevation of privilege vulnerability in Netlogon, a list of references, and a note about the references. The references list includes links to CERT-VN, CONFIRM, MISC, MLIST, and UBUNTU advisories.

**CVE-ID**  
**CVE-2020-1472** [Learn more at National Vulnerability Database \(NVD\)](#)  
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

**Description**  
An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

**References**  
**Note:** [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CERT-VN:VU#490028
- [URL:https://www.kb.cert.org/vuls/id/490028](https://www.kb.cert.org/vuls/id/490028)
- [CONFIRM:https://www.synology.com/security/advisory/Synology\\_SA\\_20\\_21](https://www.synology.com/security/advisory/Synology_SA_20_21)
- [MISC:http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html](http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html)
- [MISC:https://portal.msrmc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472](https://portal.msrmc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472)
- [URL:https://portal.msrmc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472](https://portal.msrmc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472)
- MLIST:[oss-security] 20200917 Samba and CVE-2020-1472 ("Zerologon")
- [URL:http://www.openwall.com/lists/oss-security/2020/09/17/2](http://www.openwall.com/lists/oss-security/2020/09/17/2)
- UBUNTU:USN-4510-1
- [URL:https://usn.ubuntu.com/4510-1/](https://usn.ubuntu.com/4510-1/)
- UBUNTU:USN-4510-2
- [URL:https://usn.ubuntu.com/4510-2/](https://usn.ubuntu.com/4510-2/)

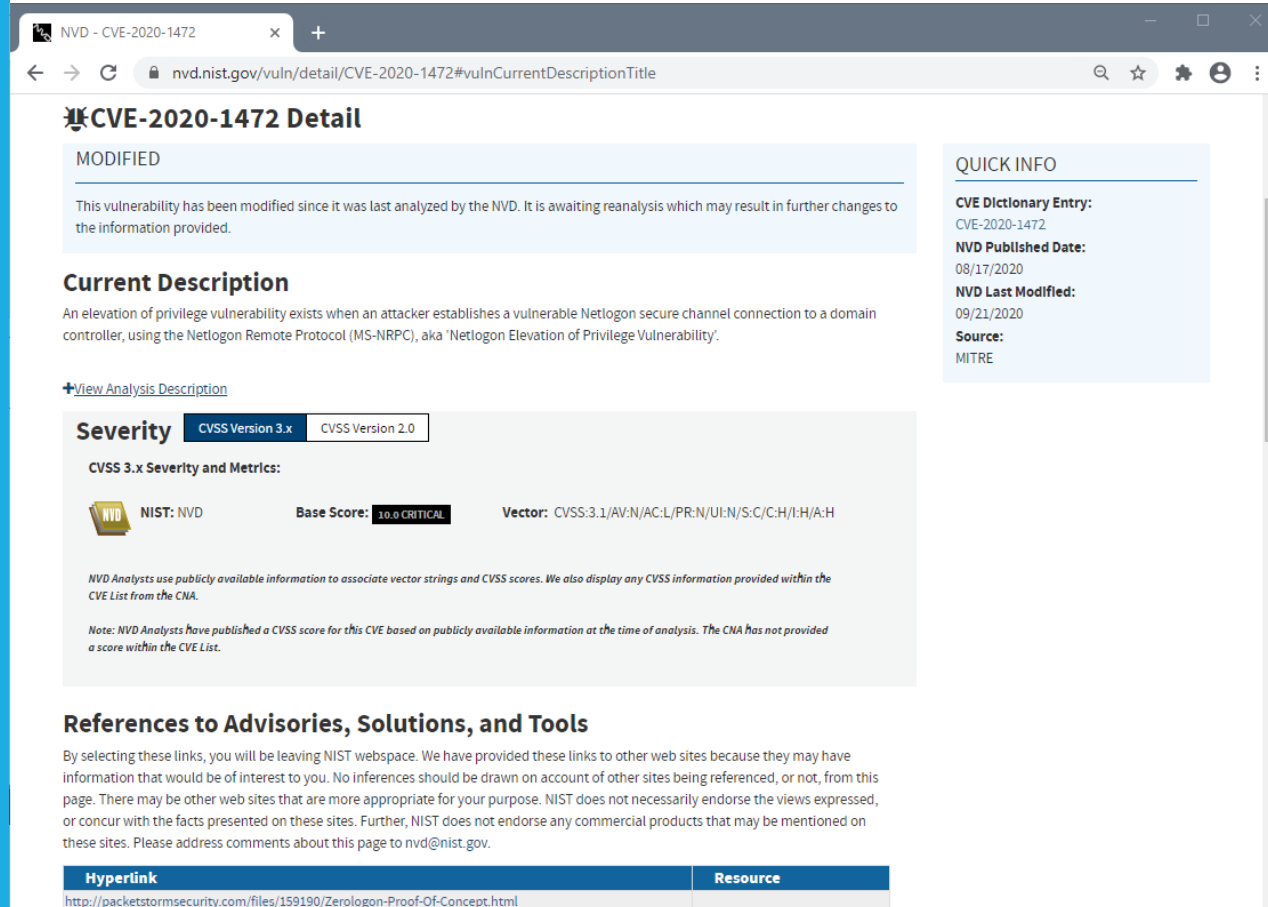
# CVE-2020-1472

## @NVD

Basic information  
about the CVE and a  
small analysis of it

The CVE Severity Score

Links to advisories,  
solutions



The screenshot shows the NIST National Vulnerability Database (NVD) page for CVE-2020-1472. The browser address bar shows the URL: [nvd.nist.gov/vuln/detail/CVE-2020-1472#vulnCurrentDescriptionTitle](https://nvd.nist.gov/vuln/detail/CVE-2020-1472#vulnCurrentDescriptionTitle). The page title is "CVE-2020-1472 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**


An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

[+View Analysis Description](#)

**Severity**

CVSS Version 3.x CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

 **NIST: NVD** **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

**References to Advisories, Solutions, and Tools**

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to [nvd@nist.gov](mailto:nvd@nist.gov).

Hypertlink	Resource
<a href="http://packetstormsecurity.com/files/159190/ZeroLogon-Proof-Of-Concept.html">http://packetstormsecurity.com/files/159190/ZeroLogon-Proof-Of-Concept.html</a>	

# 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

The screenshot shows a web browser window displaying the Microsoft Security Update Guide for CVE-2020-1472. The page title is "CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability". The URL is "portal.msrmicrosoft.com/en-US/security-guidance/advisory/CVE-2020-1472". The page is categorized under "Security Update Guide > Details".

**CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability**  
**Security Vulnerability**

Published: 08/11/2020 | Last Updated : 08/11/2020  
MITRE CVE-2020-1472

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network.

To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access.

Microsoft is addressing the vulnerability in a phased two-part rollout. These updates address the vulnerability by modifying how Netlogon handles the usage of Netlogon secure channels.

For guidelines on how to manage the changes required for this vulnerability and more information on the phased rollout, see [How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472](#).

When the second phase of Windows updates become available in Q1 2021, customers will be notified via a revision to this security vulnerability. If you wish to be notified when these updates are released, we recommend that you register for the security notifications mailer to be alerted of content changes to this advisory. See [Microsoft Technical Security Notifications](#).

**On this page**

- [Executive Summary](#)
- [Exploitability Assessment](#)
- [Security Updates](#)
- [Mitigations](#)
- [Workarounds](#)
- [FAQ](#)
- [Acknowledgements](#)
- [Disclaimer](#)
- [Revisions](#)

**Exploitability Assessment**

The following table provides an [exploitability assessment](#) for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A

[Security Updates](#) [CVSS Score](#)

# CVE-2020-1472

@Other  
places

Independent researchers  
may publish proof of  
concepts (PoC)

Very dynamic community  
with public and private  
facets

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

VoidSec/CVE-2020-1472: Exploit

github.com/VoidSec/CVE-2020-1472

Search or jump to... Pull requests Issues Marketplace Explore

VoidSec / CVE-2020-1472

Watch 4 Star 97 Fork 21

Code Issues 1 Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags

Go to file Add file Code

VoidSec Update README.md	1ba8d98 5 days ago	19 commits
research	exploit	8 days ago
.gitignore	Initial commit	8 days ago
README.md	Update README.md	5 days ago
cve-2020-1472-exploit.py	added reinstall_original_pw	7 days ago
nrpc.py	impacket patch	8 days ago
reinstall_original_pw.py	added reinstall_original_pw	7 days ago
requirements.txt	Update requirements.txt	7 days ago

README.md

## CVE-2020-1472

Checker & Exploit Code for CVE-2020-1472 aka Zerologon

Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will reset the Domain Controller's account password to an empty string.

**NOTE:** It will likely break things in production environments (eg. DNS functionality, communication with replication Domain Controllers, etc); target clients will then not be able to authenticate to the domain anymore, and they can only be re-synchronized through manual action. If you want to know more on how Zerologon attack break things, thanks to

About

Exploit Code for CVE-2020-1472 aka Zerologon

voidsec.com

exploit poc cve-2020 zerologon n-day voidsec

Readme

Releases

No releases published

Packages

No packages published

Languages

Python 100.0%

# 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

[+View Analysis Description](#)

**Severity** CVSS Version 3.x CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

 **NIST: NVD**

**Base Score:** **10.0 CRITICAL**

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Exploitability Assessment**

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A

**CVE-2020-1472**

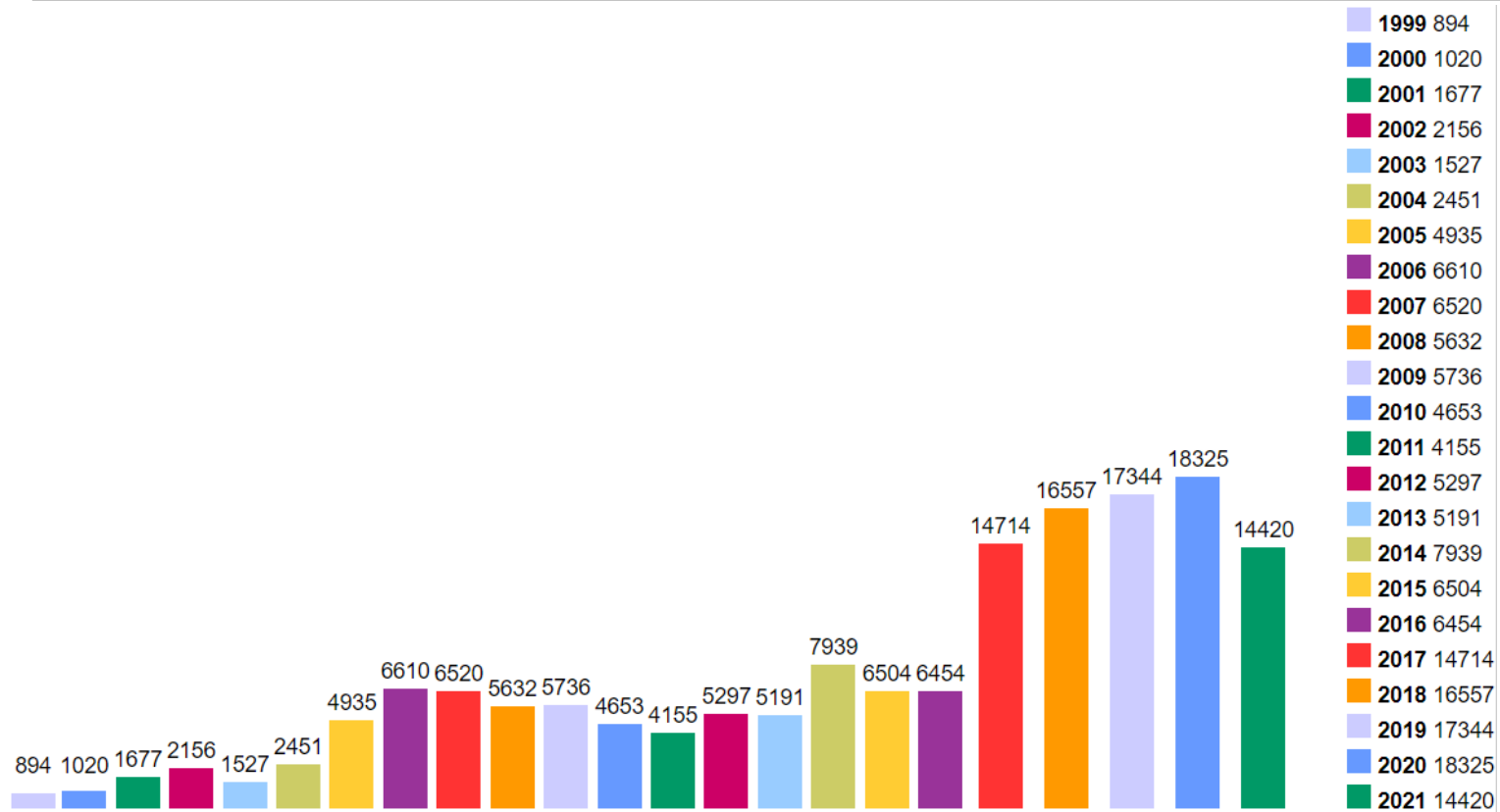
[Checker & Exploit Code for CVE-2020-1472 aka Zerologon](#)

Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will resets the Domain Controller's account password to an empty string.

**NOTE:** It will likely break things in production environments (eg. DNS functionality, communication with replication Domain Controllers, etc); target clients will then not be able to authenticate to the domain anymore, and they can only be re-synchronized through manual action. If you want to know more on how Zerologon attack break things, thanks to

# CVE per year – cvedetails.com

(as of 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

# Case Study: ShadowBrokers

---

## **Background: State actors have exploits to publicly unknown vulnerabilities**

- For many years, used for state level warfare, and never revealed

## **August 2016: Shadowbrokers publish large stash of tools from state actors**

- Use standard public channels: Twitter, Github, PasteBin, Medium
- Then several other stashes, make an auction, black friday sales, etc...
- Objective: sell tools exploiting 0 days to the highest bidder

## **March 2017: Microsoft releases patch to most Windows systems**

- but not to W7, W8, WXP and Server 2003
- Possibly tipped by state actor or researcher

# Case Study: ShadowBrokers

---

## **April 2017: ETERNALBLUE leaked by ShadowBrokers to the public**

- Exploit to MS Windows SMB v1, allowing Remote Code Execution

## **May 2017: WannaCry Ransomware**

- Uses 2 exploits from ShadowBrokers leak (ETERNALBLUE as entry point)
- Asks for \$300-600 ransom to obtain the key
- Impact: Files are encrypted in >300.000 devices

## **May 2017: EternalRocks Ransomware**

- Uses 7 exploits from ShadowBrokers leak (ETERNALBLUE as entry point)
- Impact: Panic only. Author disables worm

## **June 2017: NotPetya Ransomware**

- Variant using ETERNALBLUE and infects the Master Book Record
- Asks for \$300 ransom (but decryption key is never provided)
- Targets mostly Ukraine companies and utilities (Russia and others affected too)
- Impact: Files are lost. >\$10B of damage

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$388 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBUX

2. Send your Bitcoin wallet ID and personal installation key to e-mail: [howsmith123456@posteo.net](mailto:howsmith123456@posteo.net). Your personal installation key:

X86GcZ-7PRNBE-3mNFMp-z88VnG-uF5nhF-4wzxwZ-XdMrr6-FYG89D-xk4rNz-9

Wana Decrypt0r 2.0



Payment will be raised on

1/3/1970 17:00:00

Time Left

00:00:00:00

Your files will be lost on

1/7/1970 17:00:00

Time Left

00:00:00:00

## Ooops, your files have been encrypted!

English

### What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

 **bitcoin**  
ACCEPTED HERE

Send \$600 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Contact Us

Check Payment

Decrypt

© João Paulo Barraca

36

# Survivability

---

**How can we survive a zero-day attack?**

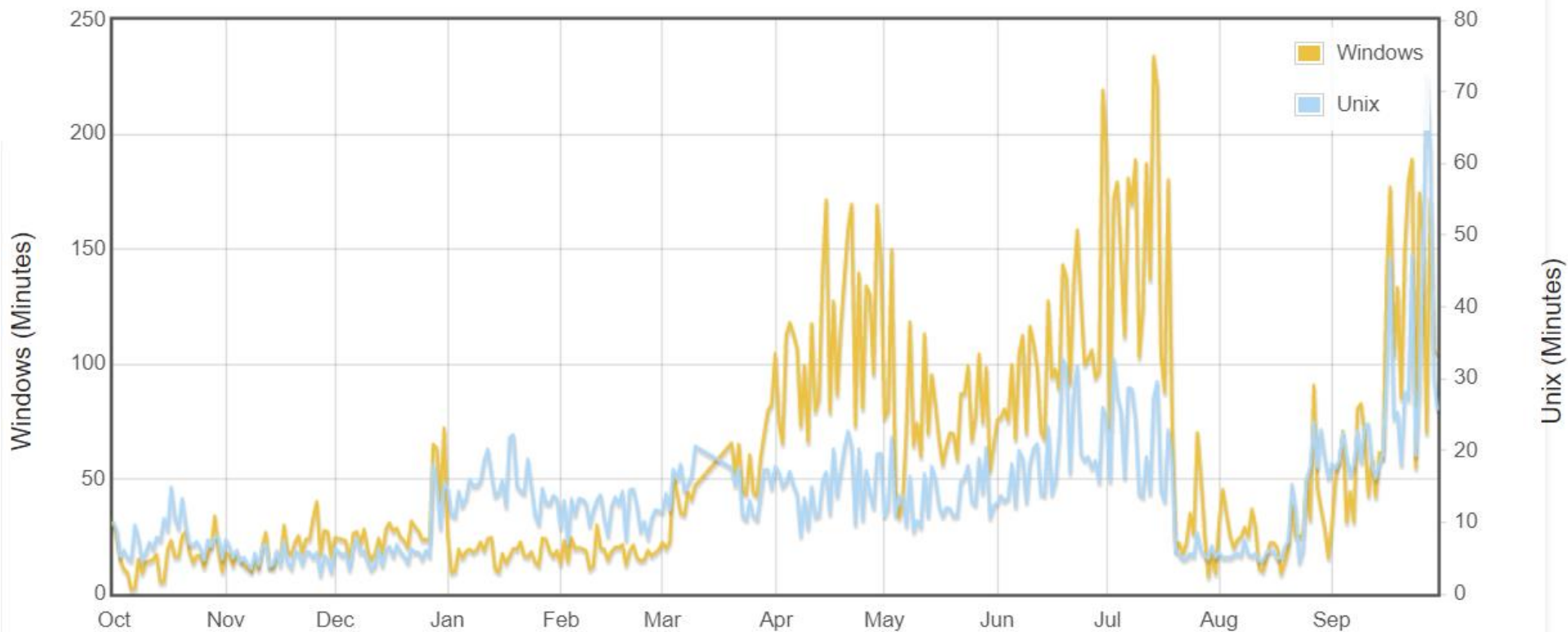
**How can we react to a massive zero-day attack?**

**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 battlefield? (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/>