Vulnerabilities

JOÃO PAULO BARRACA

Vulnerabilities

Is a weakness in a system (software, hardware…)

- It's a broad concept as a vulnerability can have multiple origins and causes

Vulnerabilities allow an attacker to violate a reasonable security policy for a system

- Policies define how a system should behave.
- Examples:
  - Wheels will turn left only when steering wheel turns left
  - Phones will only allow access to its owner
  - Programs will only run code inserted by its original developer

Vulnerability number always increases as software grows

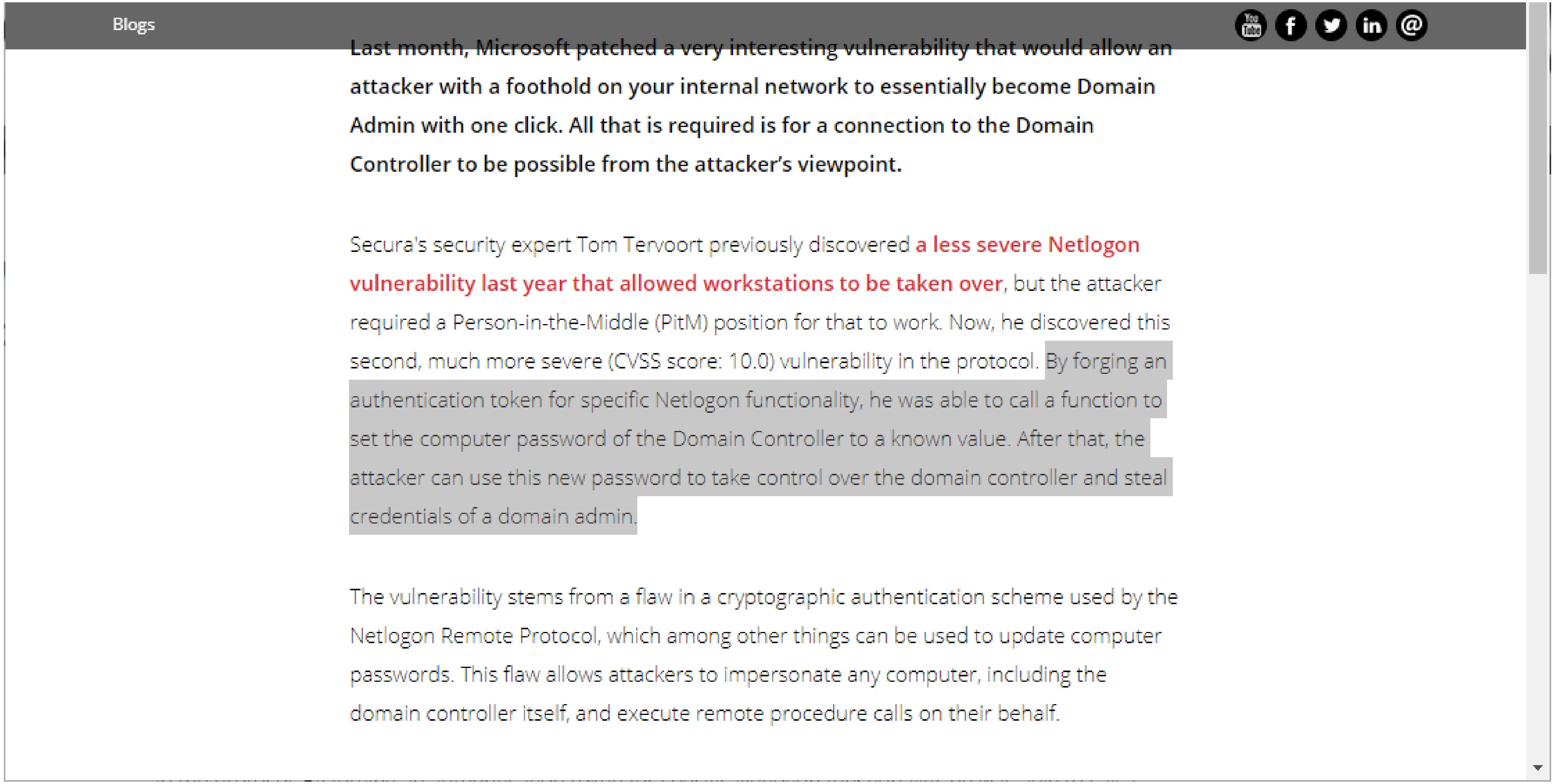
- It's inherent to the increased complexity, interactions, development process
- Also, they do not disappear
- Software is updated with fixes, but older software is still vulnerable

Vulnerabilities

Vulnerabilities are states in a computing system that either allows an attacker to:

1. execute commands as another user
2. access data that is contrary to the specified access restrictions for that data
3. pose as another entity
4. conduct a denial of service (DoS) (affect availability)

A simple vulnerability - secura.com



Last month, Microsoft patched a very interesting vulnerability that would allow an attacker with a foothold on your internal network to essentially become Domain Admin with one click. All that is required is for a connection to the Domain Controller to be possible from the attacker's viewpoint.

Secura's security expert Tom Tervoort previously discovered **a less severe Netlogon vulnerability last year that allowed workstations to be taken over**, but the attacker required a Person-in-the-Middle (PitM) position for that to work. Now, he discovered this second, much more severe (CVSS score: 10.0) vulnerability in the protocol. By forging an authentication token for specific Netlogon functionality, he was able to call a function to set the computer password of the Domain Controller to a known value. After that, the attacker can use this new password to take control over the domain controller and steal credentials of a domain admin.

The vulnerability stems from a flaw in a cryptographic authentication scheme used by the Netlogon Remote Protocol, which among other things can be used to update computer passwords. This flaw allows attackers to impersonate any computer, including the domain controller itself, and execute remote procedure calls on their behalf.

CIA triad – What vulnerabilities directly impact

Confidentiality

- Whether information is disclosed to others

Integrity

- Whether data contents and formats are kept safe from modifications

Availability

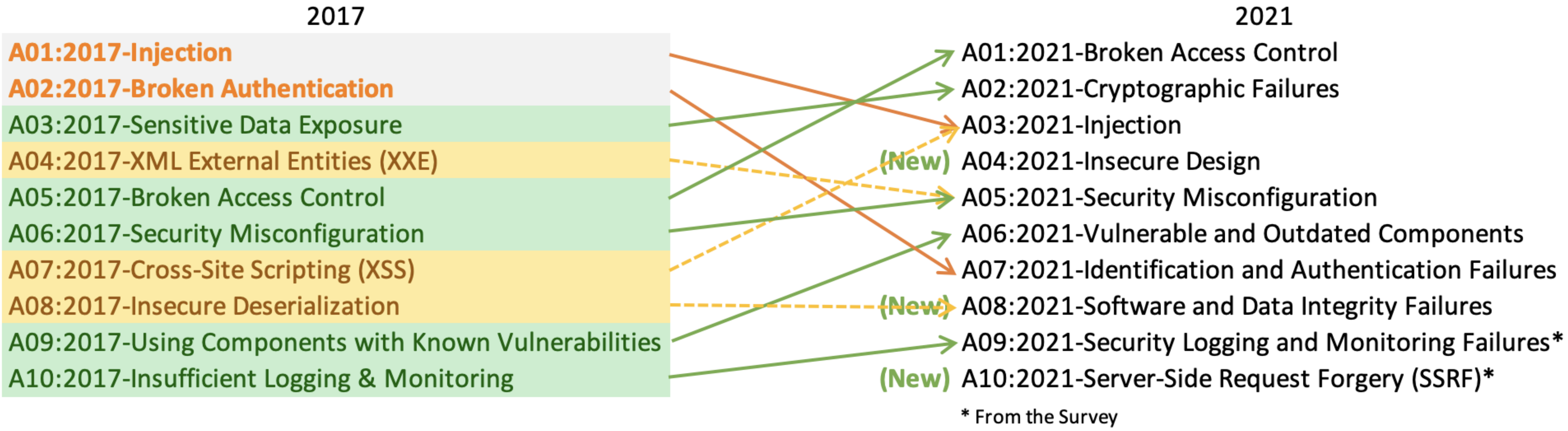
- Whether system performance is degraded

Vulnerability sources – OWASP Top 10 (Web)

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

List of the Most Prevalent Sources of Vulnerabilities, as determined by the community. Reevaluated every 3-5 years.

Vulnerability sources – OWASP Top 10 (Web)



2017

- **A01:2017-Injection**
- **A02:2017-Broken Authentication**
- A03:2017-Sensitive Data Exposure
- A04:2017-XML External Entities (XXE)
- A05:2017-Broken Access Control
- A06:2017-Security Misconfiguration
- A07:2017-Cross-Site Scripting (XSS)
- A08:2017-Insecure Deserialization
- A09:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- (New) A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- (New) A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- (New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Vulnerability sources – 7 Pernicious Kingdoms

1. **Input Validation and Representation**
2. **API Abuse**
3. **Security Features**
4. **Time and State**
5. **Errors**
6. **Code Quality**
7. **Encapsulation**

***. Environment**

K. Tsipenyuk, B. Chess and G. McGraw, "Seven pernicious kingdoms: a taxonomy of software security errors," in IEEE Security & Privacy, vol. 3, no. 6, pp. 81-84, Nov.-Dec. 2005, doi: 10.1109/MSP.2005.159.

Vulnerability sources - CWE

Vulnerabilities may exist due to Bugs or Faults

- Bug is an error in the implementation of a software
- Fault is a design or architectural error

CWE - Common Weaknesses Enumeration

- Extensive (944) list of anti-patterns that may lead to insecure systems
- Organized in a tree, with examples in multiple languages

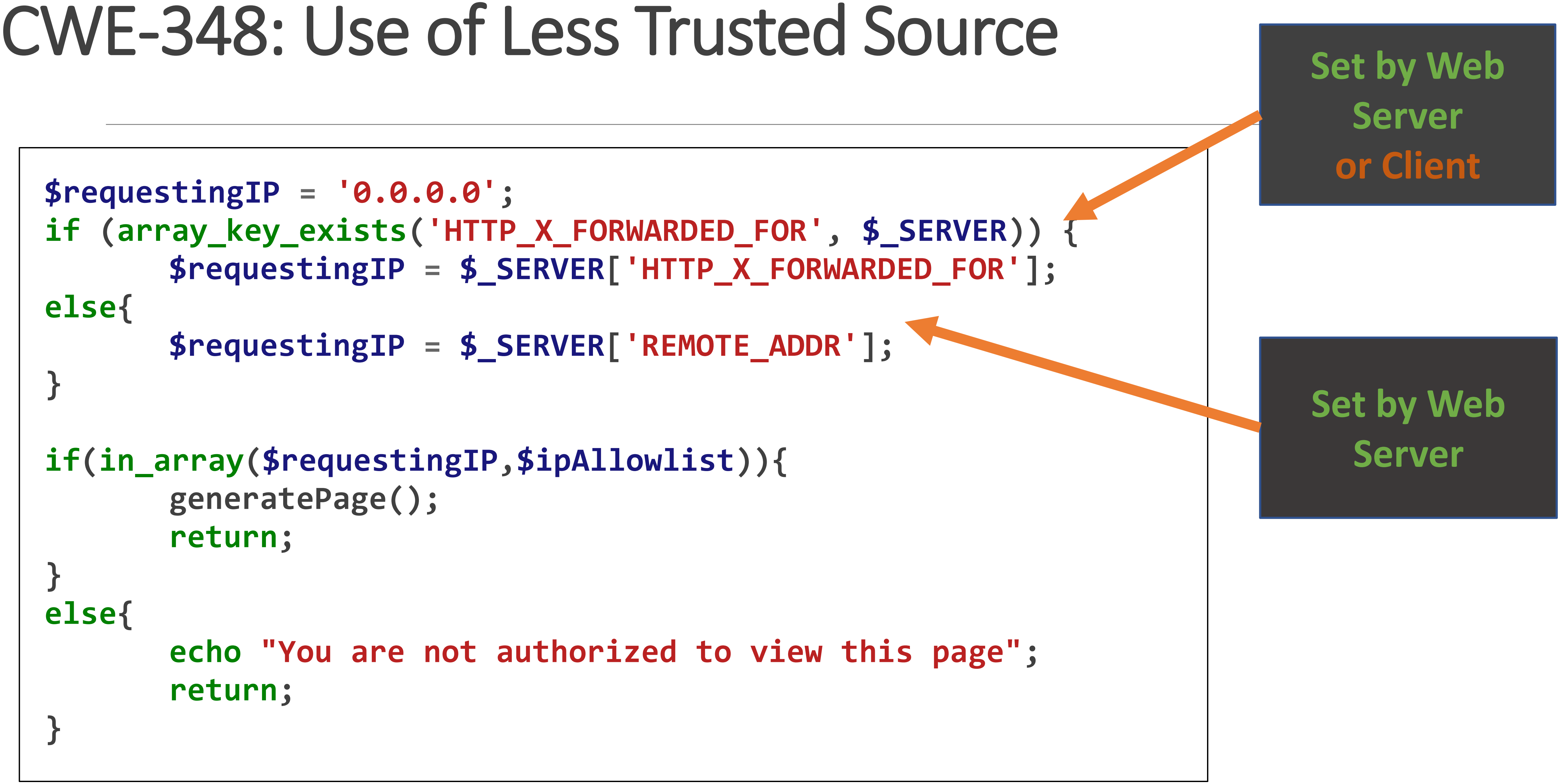
CWE-348: Use of Less Trusted Source

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

Vulnerability Tracking by vendors

During the development cycle, vulnerabilities are handled as bugs

- May have be handled by a security team or not
- May have a security classification and SLA

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

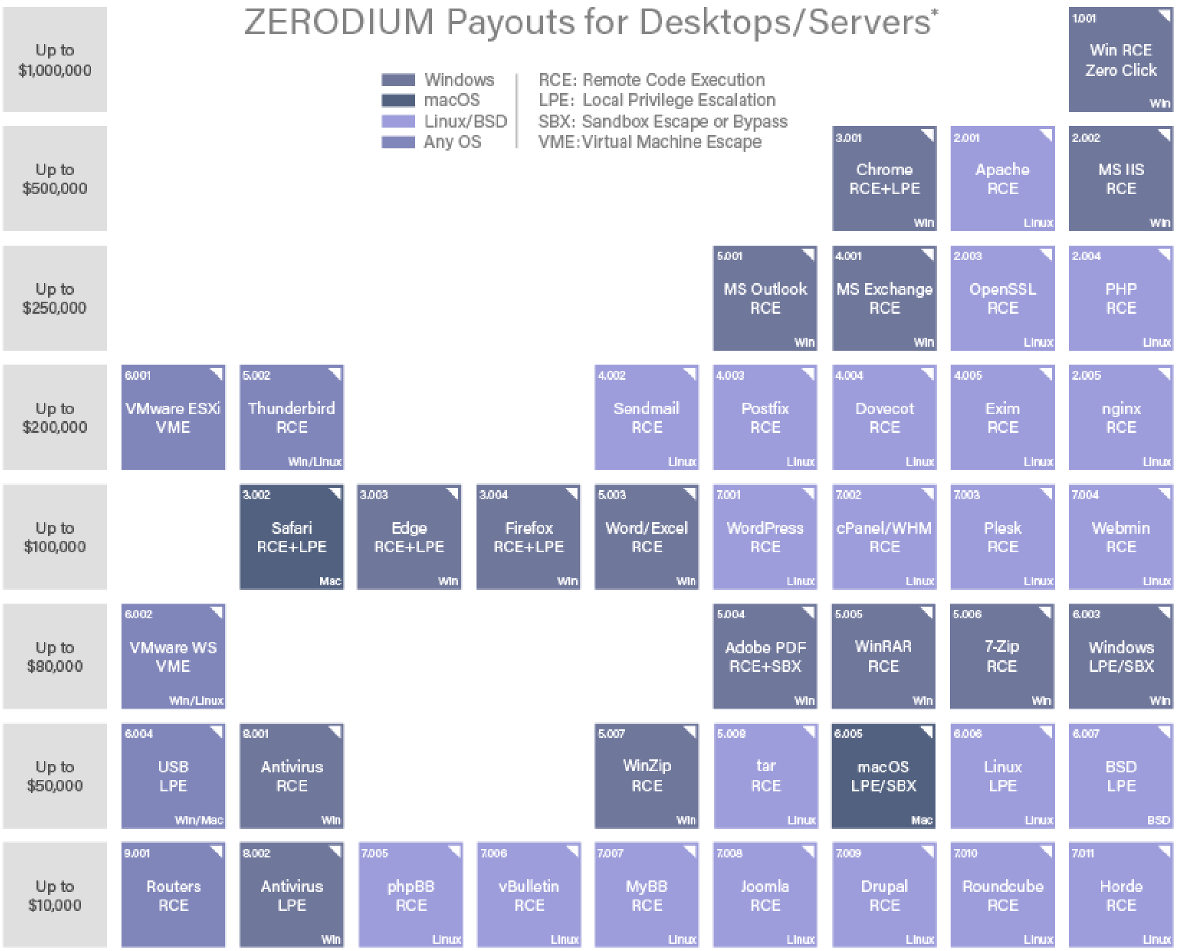
- Constitute an arsenal for future attacks against targets
- Exploits can be considered as assets in cyberwar

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)
  - 5M€: 1 click Android exploit
  - 5 to 7M€: 1 click iPhone exploit
  - 2 to 3M€: Chrome RCE + LPE exploit (Mobile)
  - 1.5M€: Chrome Desktop
  - Many others (E.g. https://www.crowdfense.com/exploit-acquisition-program/)

…and privately traded at unknown prices

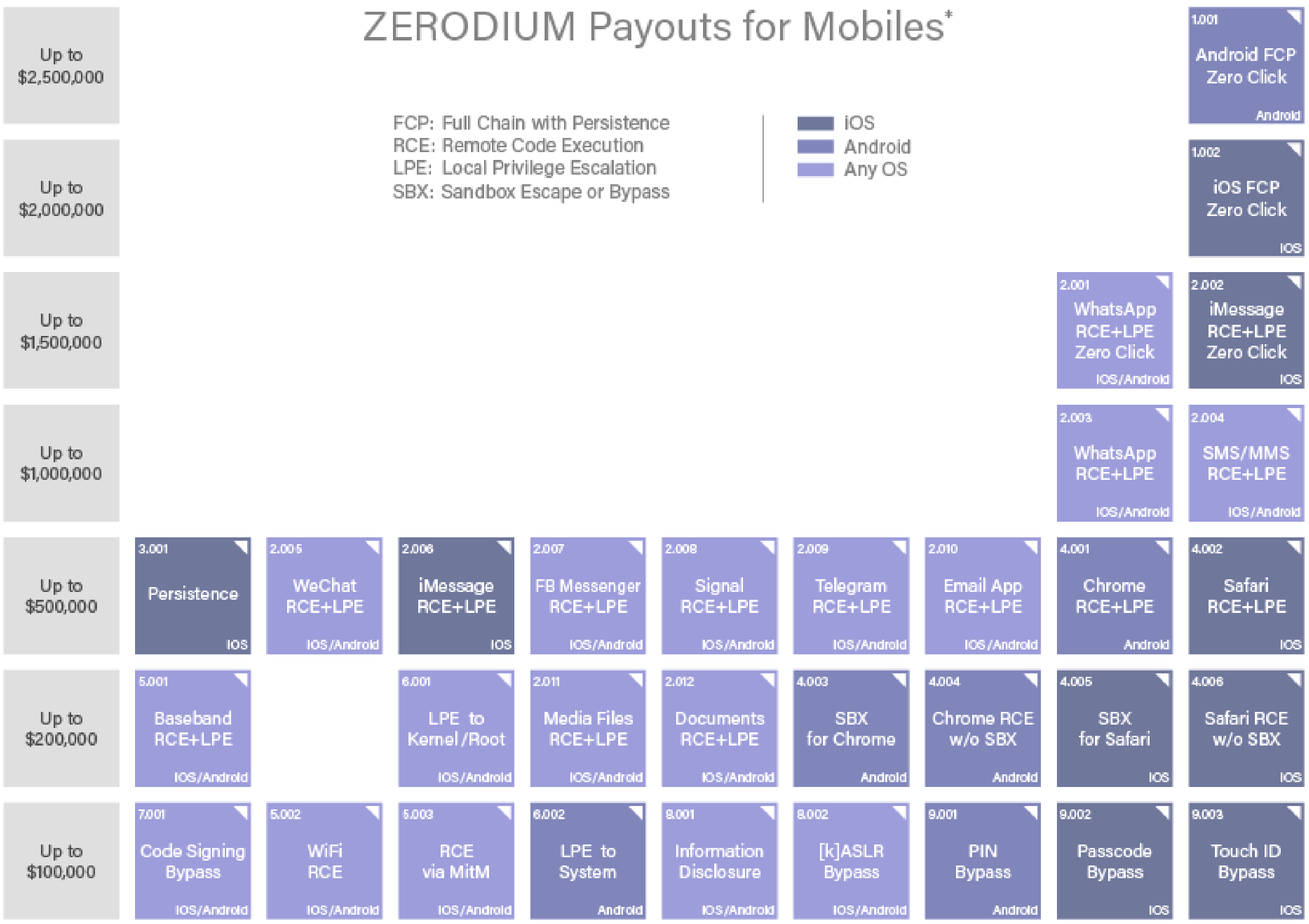
- Private Companies, Organized Crime, APTs



ZERODIUM Payouts for Desktops/Servers*

▨ Windows	RCE: Remote Code Execution
▨ macOS	LPE: Local Privilege Escalation
▨ Linux/BSD	SBX: Sandbox Escape or Bypass
▨ Any OS	VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence	▨ iOS
RCE: Remote Code Execution	▨ Android
LPE: Local Privilege Escalation	▨ Any OS
SBX: Sandbox Escape or Bypass	

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

Source, https://zerodium.com/program.html

Vulnerability Tracking

Most well-known trackers systems: CVE and NVD

- CVE: Common Vulnerabilities and Exposures, managed by MITRE
- NVD: National Vulnerability Database, managed by NIST
  - Fed by CVE@MITRE but provides enhanced information

Others

- CERT Vulnerability Notes Database (VNDB)
  - Maintained by CERTs, may provide additional information regarding a CVE
- VulnDB
  - Focus on APIs and providing information to companies
- DISA IAVA and STIGS
  - Information Assurance Vulnerability Alerts: includes MIL and GOV systems
  - Security Technical Implementation Guides
- Industry Sharing and Analysis Centers (ISAC)
  - Industry driven, thematic (AUTO, FINANTIAL, IT, etc… groups)

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

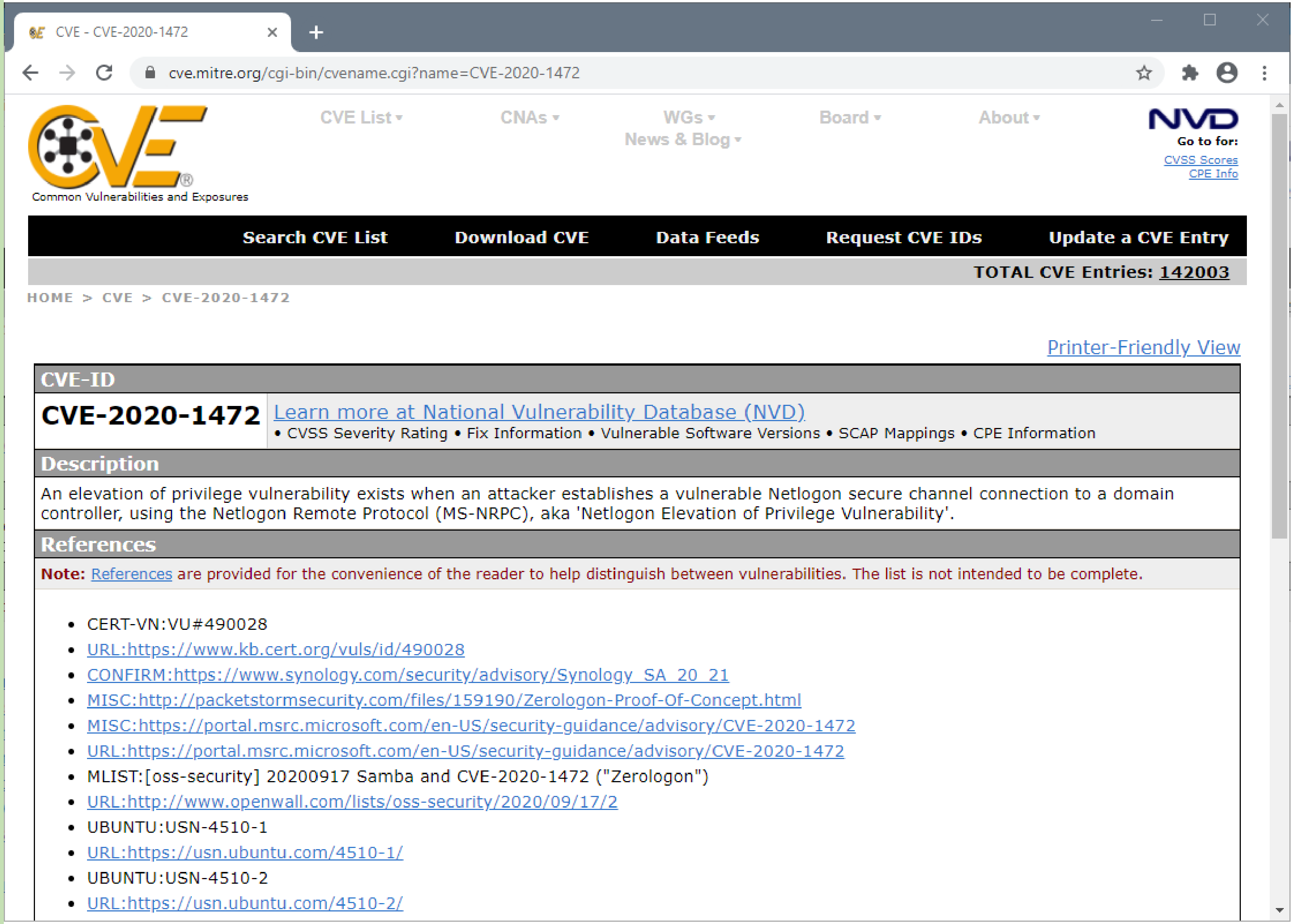
- Part of responsible disclosure: Until owner provides a fix

CVE-2020-1472

@MITRE

Basic information about the CVE

References to other trackers (provided for convenience)



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
- CONFIRM:https://www.synology.com/security/advisory/Synology_SA_20_21
- MISC:http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html
- MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
- URL:https://portal.msrc.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
- UBUNTU:USN-4510-1
- URL:https://usn.ubuntu.com/4510-1/
- UBUNTU:USN-4510-2
- URL:https://usn.ubuntu.com/4510-2/

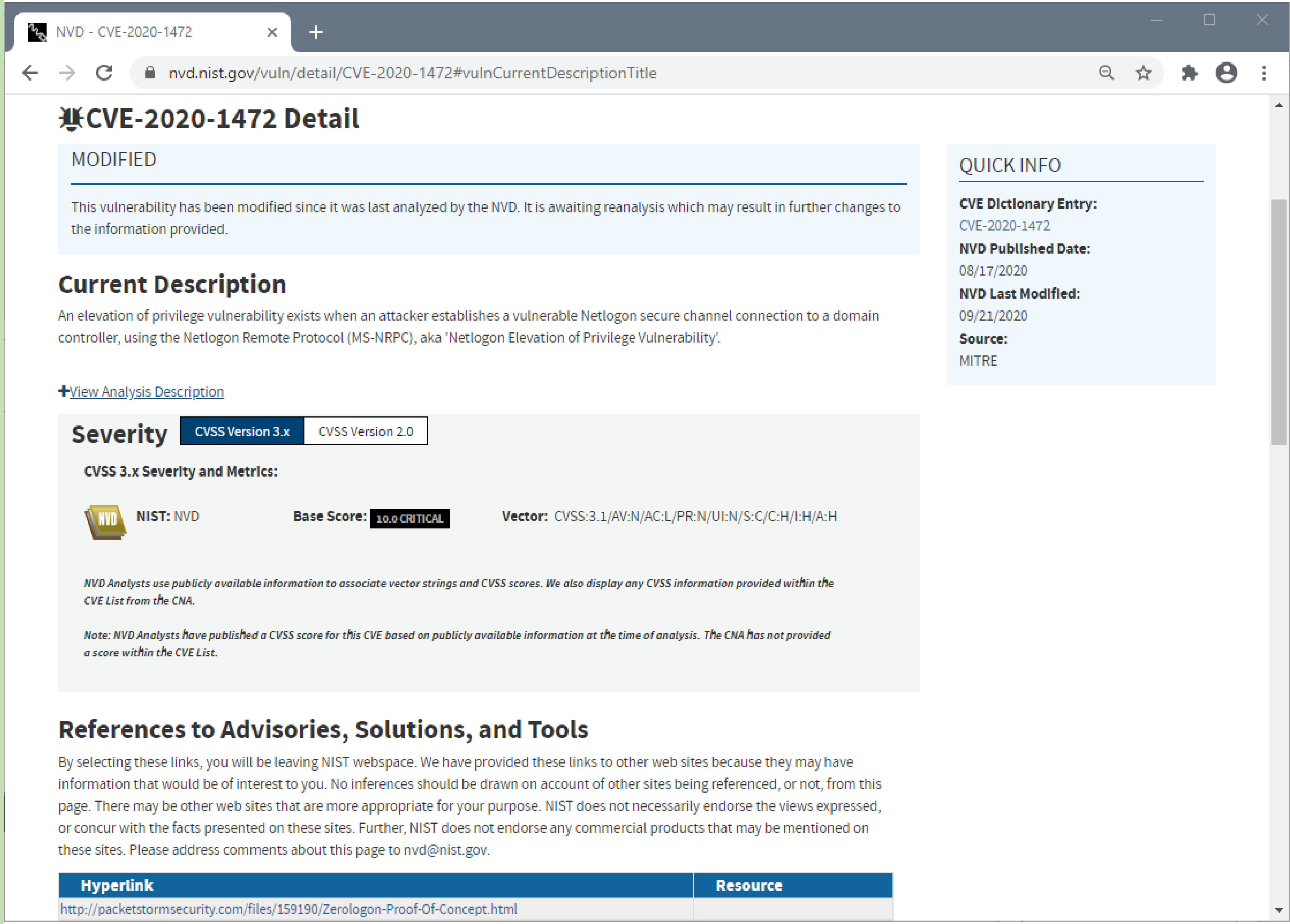
CVE-2020-1472

@NVD

Basic information about the CVE and a small analysis of it

The CVE Severity Score

Links to advisories, solutions



NVD - CVE-2020-1472
nvd.nist.gov/vuln/detail/CVE-2020-1472#vulnCurrentDescriptionTitle

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.

Hyperlink	Resource
http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html	

QUICK INFO

CVE Dictionary Entry:
CVE-2020-1472
NVD Published Date:
08/17/2020
NVD Last Modified:
09/21/2020
Source:
MITRE

CVE-2020-1472

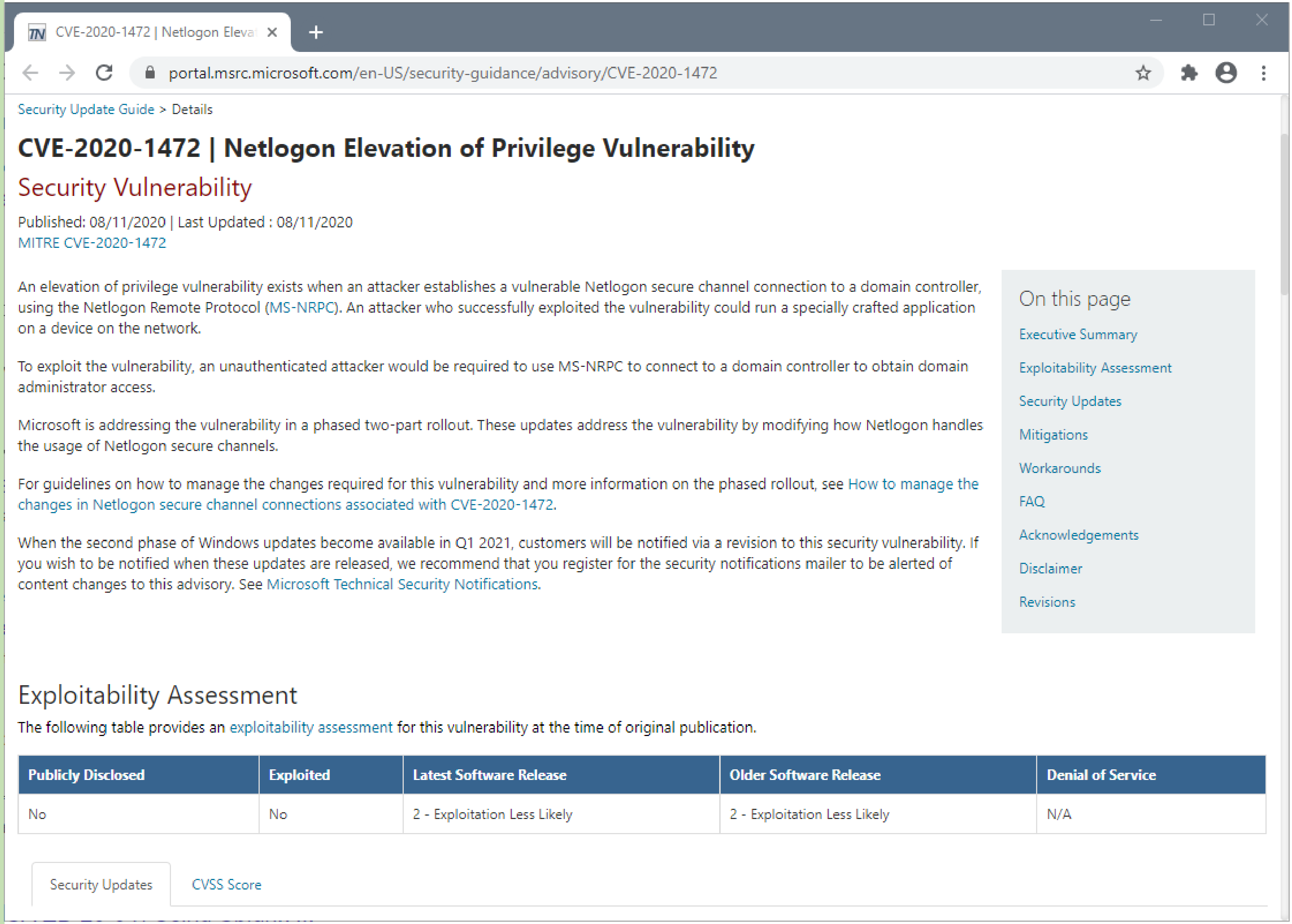
@Product Owner

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 | Netlogon Eleva
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
Security Update Guide > Details
On this page
Executive Summary
Exploitability Assessment
Security Updates
Mitigations
Workarounds
FAQ
Acknowledgements
Disclaimer
Revisions
Security Updates
CVSS Score

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.

Exploitability Assessment

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

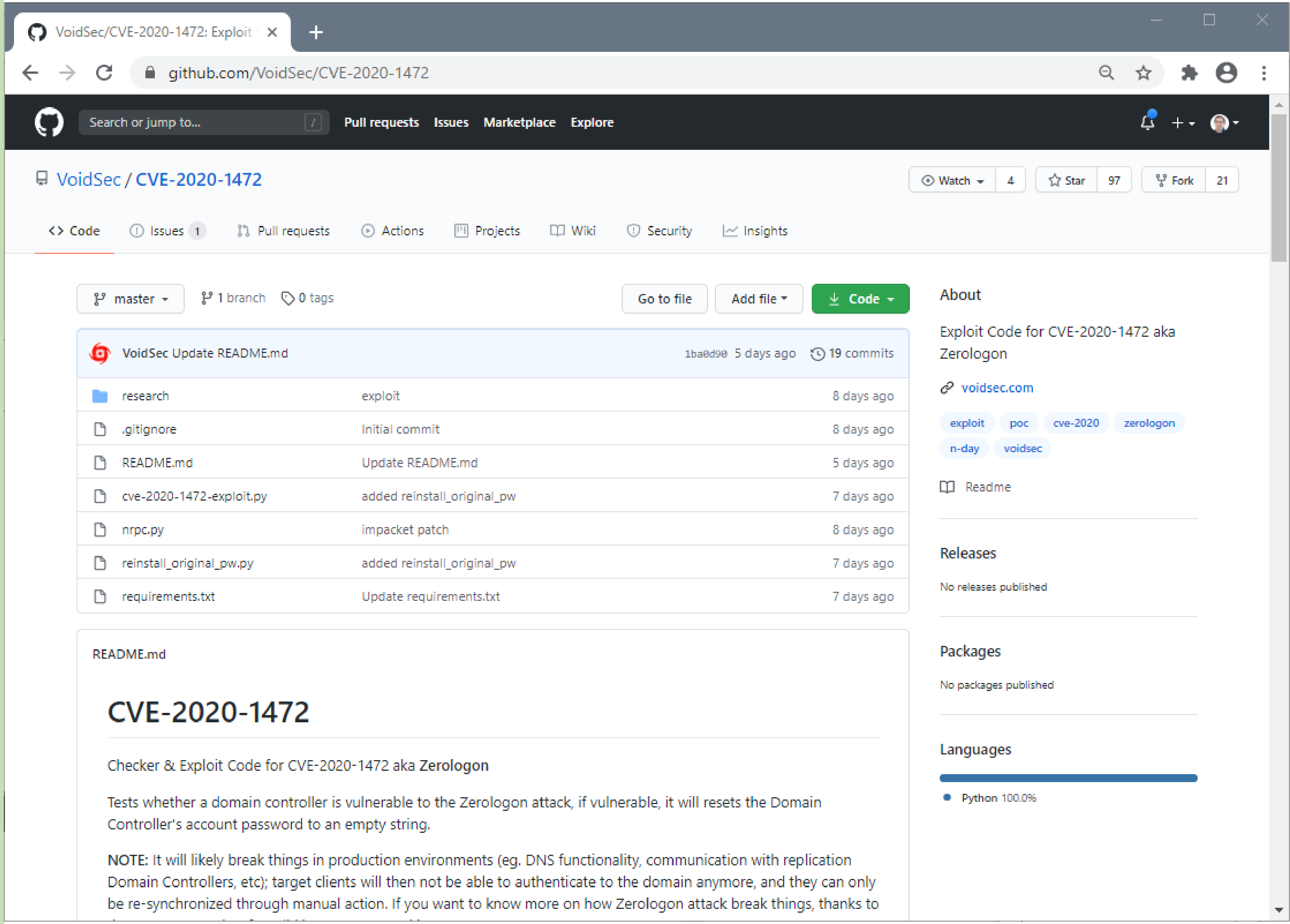
Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A

CVE-2020-1472

@Other places

Independent researchers may publish validation tools or exploits

Very dynamic community with public and private facets



VoidSec Update README.md 1ba0d90 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

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%

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 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

Vulnerability tracking

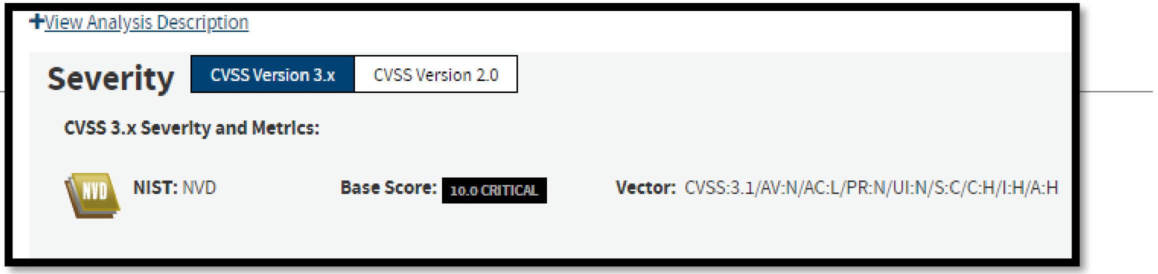
Not an easy task

- 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

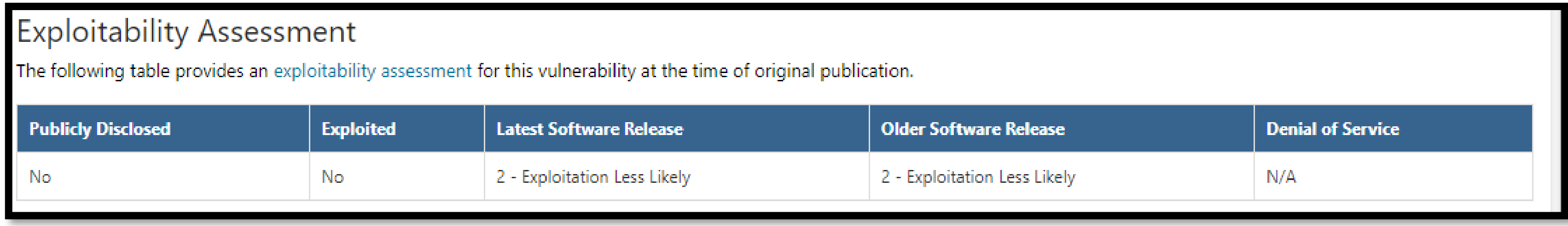


+View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

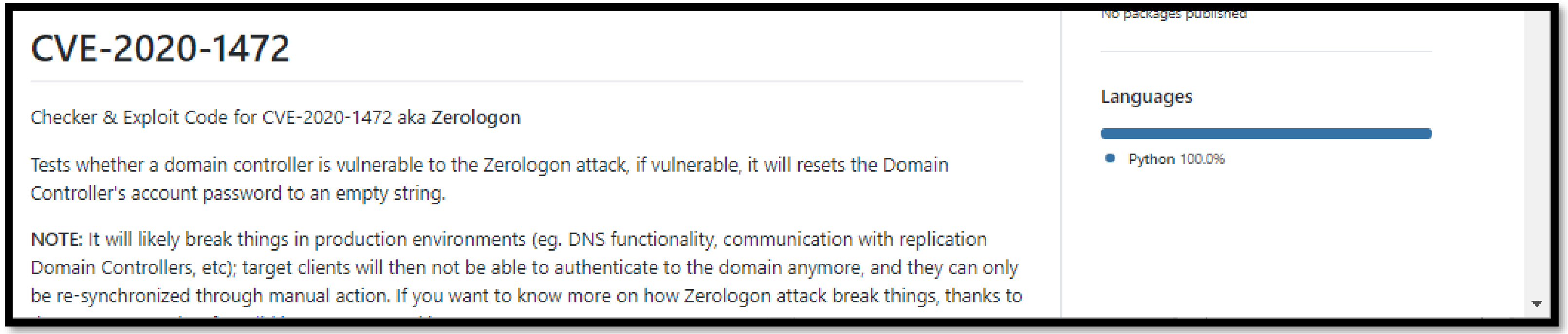
NIST: NVD **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



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.

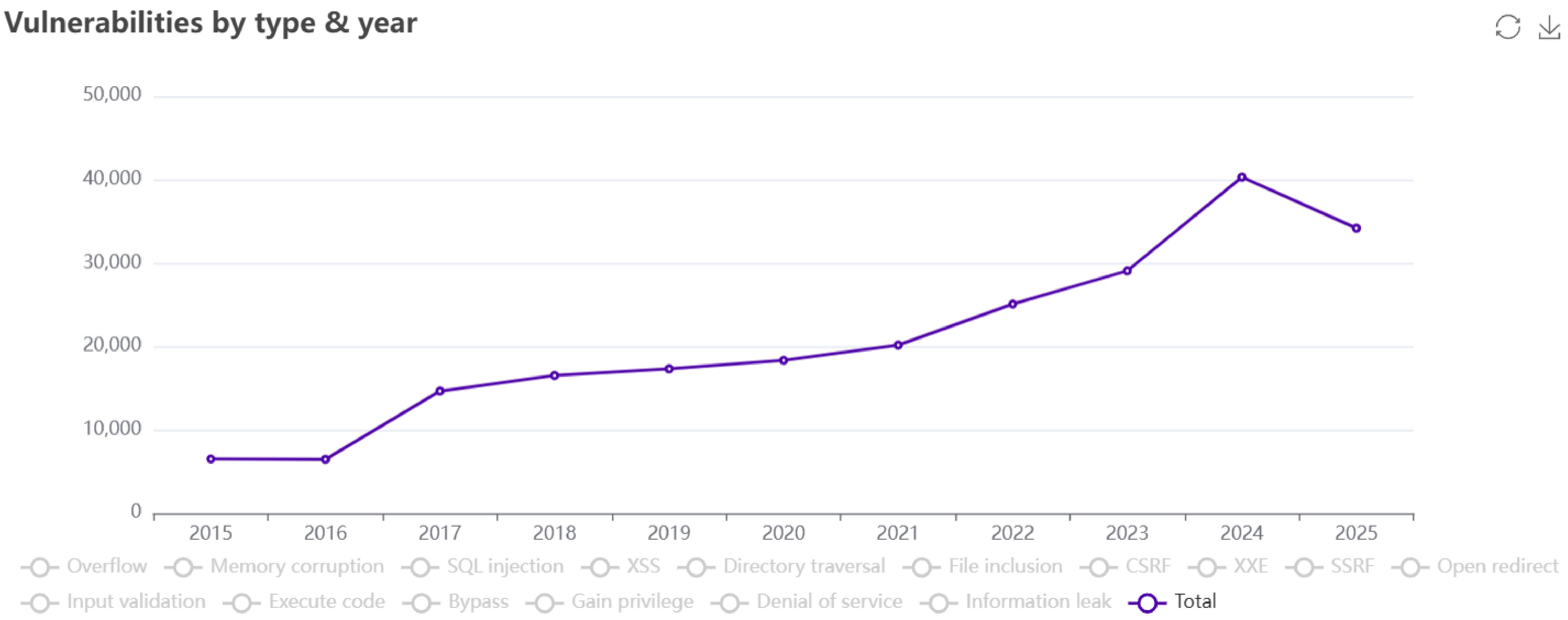
NOTE: It will likely break things in production environments (eg. DNS functionality, communication with replication Domain Controllers, etc); target clients will then not be able to authenticate to the domain anymore, and they can only be re-synchronized through manual action. If you want to know more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

No packages published

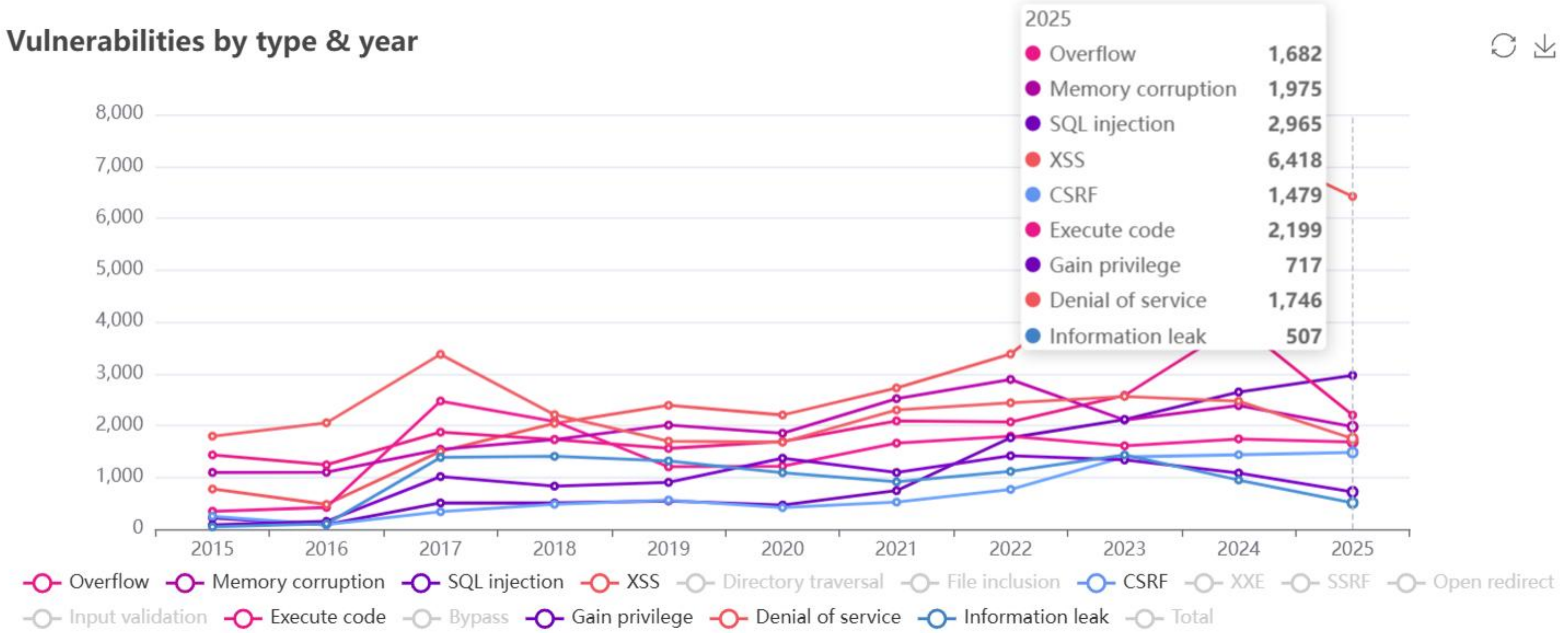
Languages

● Python 100.0%

CVE per year – cvedetails.com (as of Sep 2025)



CVE per year – cvedetails.com (as of Sep 2025)



Vulnerabilities by type & year

2025	
● Overflow	1,682
● Memory corruption	1,975
● SQL injection	2,965
● XSS	6,418
● CSRF	1,479
● Execute code	2,199
● Gain privilege	717
● Denial of service	1,746
● Information leak	507

CVSS – Common Vulnerability Scoring System

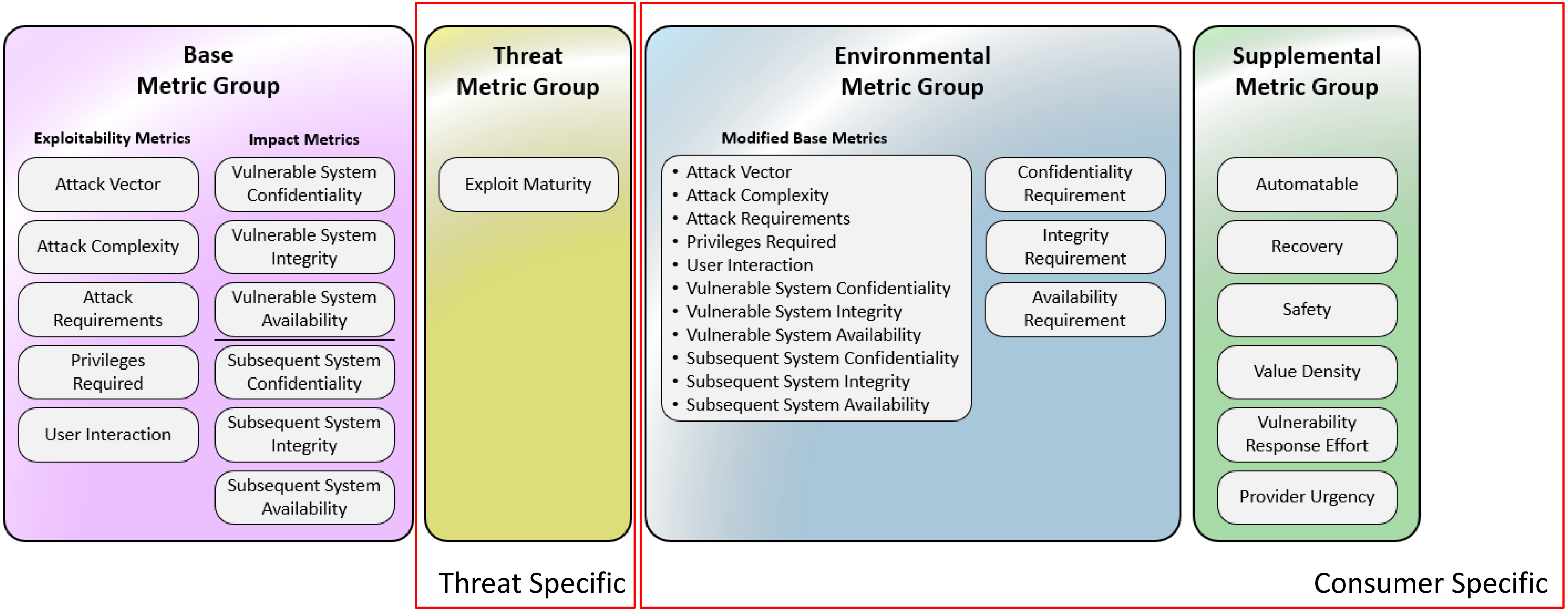
Provides a quick way to determine the severity of a vulnerability (0-10 score)

- Helps defenders prioritizing the deployment of mitigations
- Helps attackers selecting the most convenient vulnerability to explore
- Tends to be pessimistic (higher values)

Example: 7.3 - CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	Present	Multiple conditions that require target specific reconnaissance and preparation must be satisfied in order to achieve successful exploitation of this vulnerability.
Privileges Required	Low	An attacker must be able to place a file within the web root to be processed by NGINX.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Vulnerable System Integrity	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Vulnerable System Availability	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Subsequent System Confidentiality	None	There is no impact to the subsequent system confidentiality.
Subsequent System Integrity	None	There is no impact to the subsequent system integrity.
Subsequent System Availability	None	There is no impact to the subsequent system availability.

CVSS – Common Vulnerability Scoring System



CVSS – Common Vulnerability Scoring System

Base metrics

- Metric intrinsic to the vulnerability
- How exploitable it is
- What is the potential impact

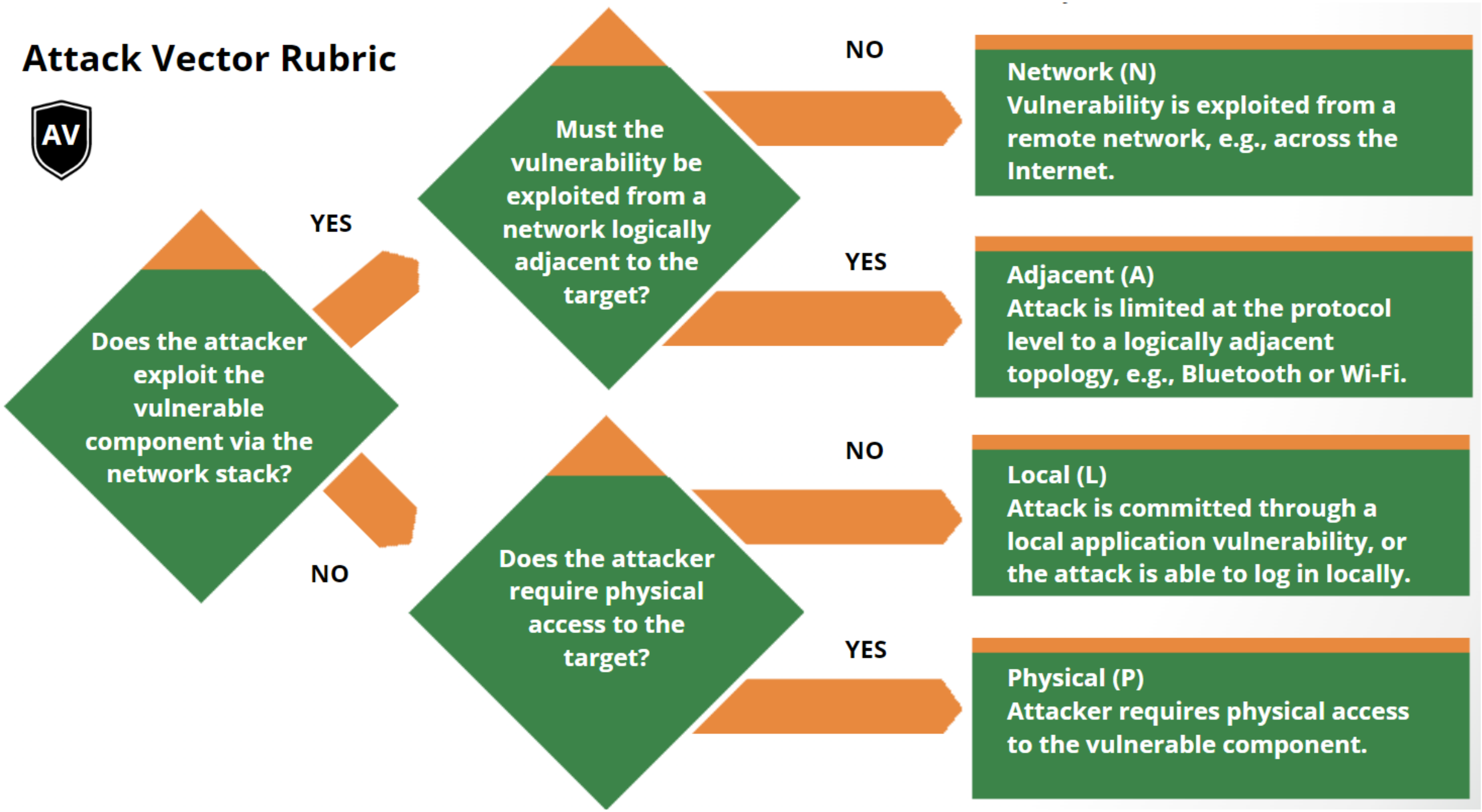
Threat metrics

- What is the current situation regarding the support for its exploitability
- Existence of PoC, active exploits, active campaigns

Environmental metrics

- What is the actual situation at each customer
  - How it really impacts the system operation, and what are the system requirements
- How the vulnerability is relevant to the customer and its clients

CVSS – Common Vulnerability Scoring System



Attack Vector Rubric

AV

Does the attacker exploit the vulnerable component via the network stack?

YES

Must the vulnerability be exploited from a network logically adjacent to the target?

NO

Network (N)
Vulnerability is exploited from a remote network, e.g., across the Internet.

YES

Adjacent (A)
Attack is limited at the protocol level to a logically adjacent topology, e.g., Bluetooth or Wi-Fi.

NO

Does the attacker require physical access to the target?

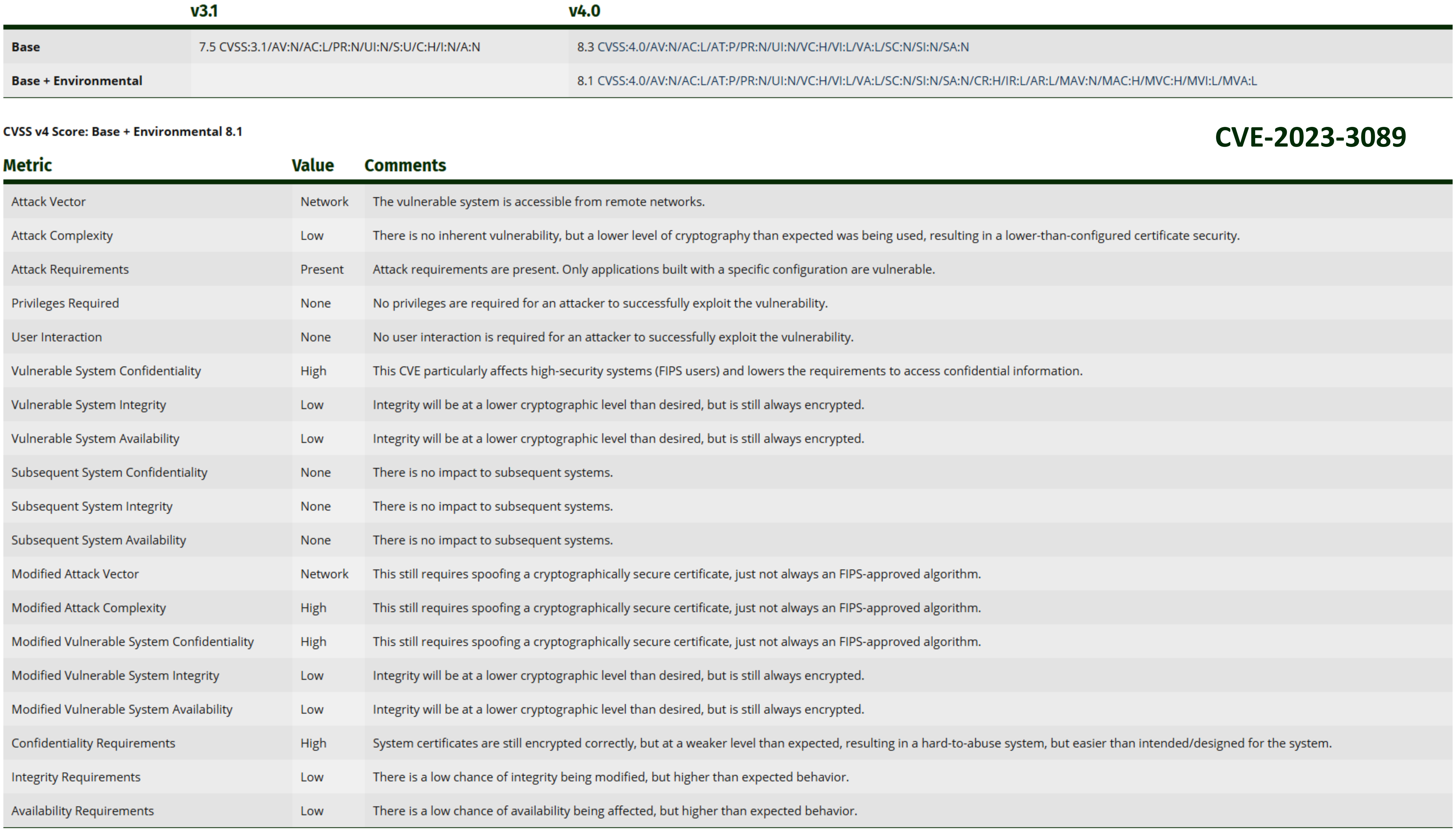
NO

Local (L)
Attack is committed through a local application vulnerability, or the attack is able to log in locally.

YES

Physical (P)
Attacker requires physical access to the vulnerable component.

CVE-2023-3089



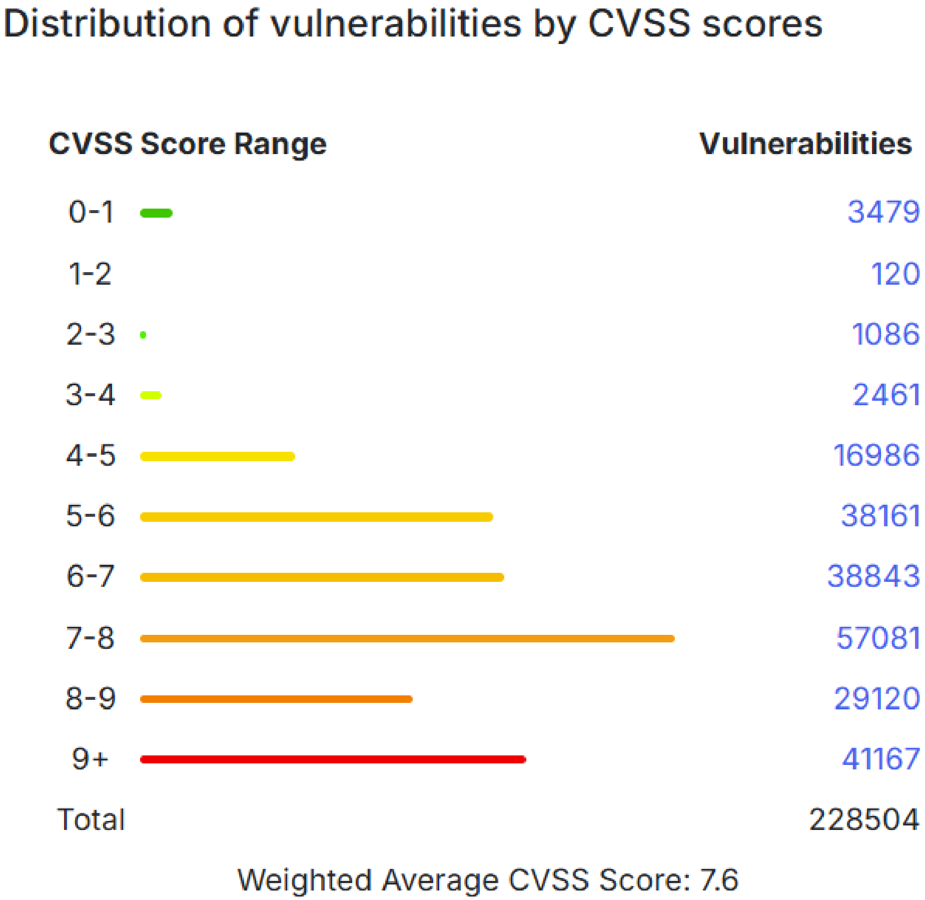
	v3.1	v4.0
Base	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	8.3 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N
Base + Environmental		8.1 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N/CR:H/IR:L/AR:L/MAV:N/MAC:H/MVC:H/MVI:L/MVA:L

CVSS v4 Score: Base + Environmental 8.1

Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	There is no inherent vulnerability, but a lower level of cryptography than expected was being used, resulting in a lower-than-configured certificate security.
Attack Requirements	Present	Attack requirements are present. Only applications built with a specific configuration are vulnerable.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	This CVE particularly affects high-security systems (FIPS users) and lowers the requirements to access confidential information.
Vulnerable System Integrity	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Vulnerable System Availability	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Subsequent System Confidentiality	None	There is no impact to subsequent systems.
Subsequent System Integrity	None	There is no impact to subsequent systems.
Subsequent System Availability	None	There is no impact to subsequent systems.
Modified Attack Vector	Network	This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm.
Modified Attack Complexity	High	This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm.
Modified Vulnerable System Confidentiality	High	This still requires spoofing a cryptographically secure certificate, just not always an FIPS-approved algorithm.
Modified Vulnerable System Integrity	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Modified Vulnerable System Availability	Low	Integrity will be at a lower cryptographic level than desired, but is still always encrypted.
Confidentiality Requirements	High	System certificates are still encrypted correctly, but at a weaker level than expected, resulting in a hard-to-abuse system, but easier than intended/designed for the system.
Integrity Requirements	Low	There is a low chance of integrity being modified, but higher than expected behavior.
Availability Requirements	Low	There is a low chance of availability being affected, but higher than expected behavior.

CVSS – Common Vulnerability Scoring System

Risk Ranking	CVSS Score	SLA in days
Critical	8.0 – 10.0	15
High	6.0 – 7.9	30
Medium	4.0 – 5.9	90
Low	2.0 – 3.9	180
Very Low	0.0 – 1.9	360



Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	3479
1-2	120
2-3	1086
3-4	2461
4-5	16986
5-6	38161
6-7	38843
7-8	57081
8-9	29120
9+	41167
Total	228504

Weighted Average CVSS Score: 7.6

Vulnerability Management must consider CVSS , customer capability to remediation and product

Vulnerability Disclosure

How should a research proceed when a vulnerability is found?

If the engagement is private: <u>deliver to contracting entity</u>

- May negotiate the public release the information…
- Commonly handled under a Non-Disclosure Agreement (NDA)

What about other cases?

Vulnerability Disclosure: None

Researcher doesn’t notify vendor about vulnerability

- Doesn’t care
- Uses it as part of an arsenal or trades the information

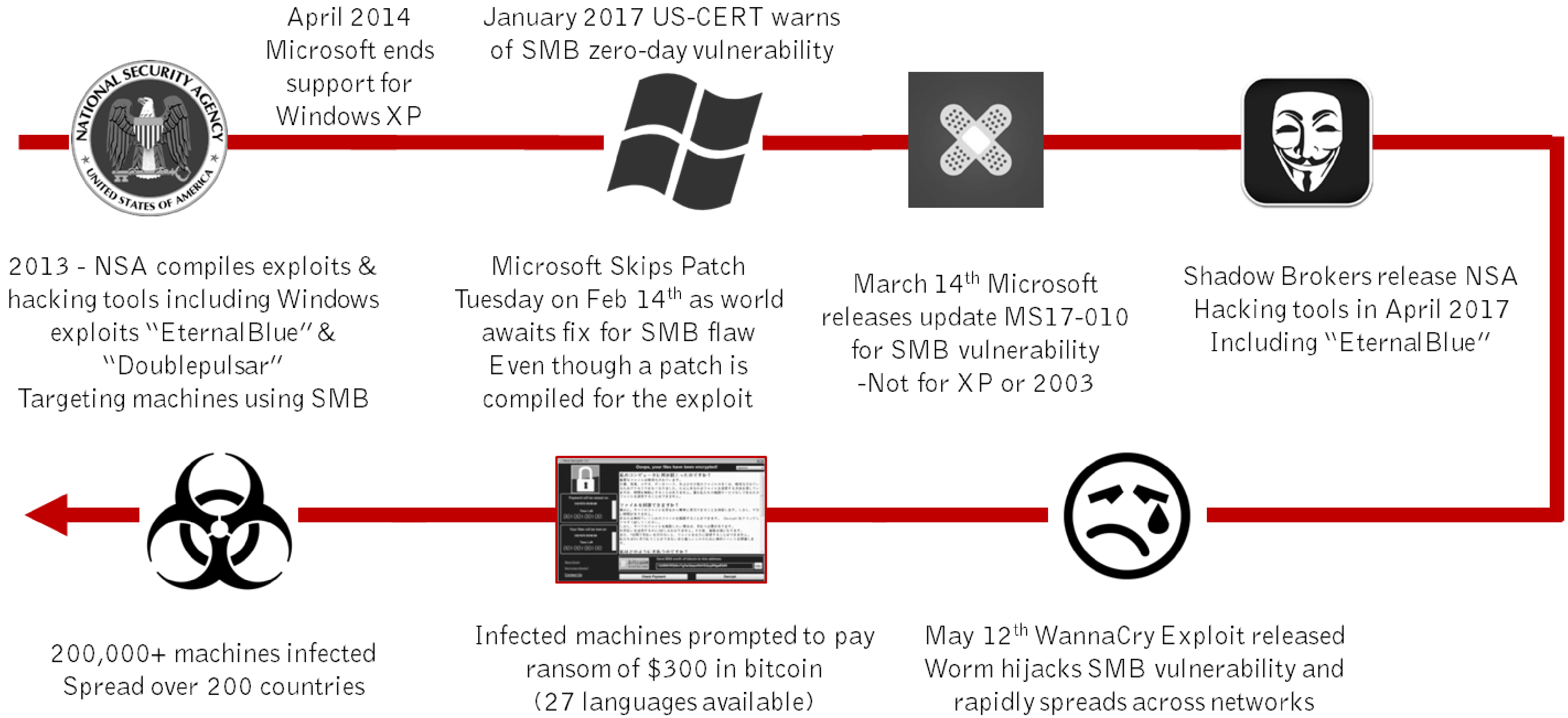
Leads to 0-day vulnerabilities

- Vulnerability is not known to the public and there is no direct remediation
- Some other third parties may also know about the vulnerability and exploit it

If impact is high, it creates major disruption when publicly known

- Quick adoption in malware and dissemination
  - Remember: Systems take at least one month to be patched

CVE-2017-0144 EternalBlue



2013 - NSA compiles exploits & hacking tools including Windows exploits "EternalBlue" & "Doublepulsar"
Targeting machines using SMB

April 2014
Microsoft ends support for Windows XP

January 2017 US-CERT warns of SMB zero-day vulnerability

Microsoft Skips Patch Tuesday on Feb 14th as world awaits fix for SMB flaw
Even though a patch is compiled for the exploit

March 14th Microsoft releases update MS17-010 for SMB vulnerability
-Not for XP or 2003

Shadow Brokers release NSA Hacking tools in April 2017
Including "EternalBlue"

May 12th WannaCry Exploit released
Worm hijacks SMB vulnerability and rapidly spreads across networks

Infected machines prompted to pay ransom of $300 in bitcoin
(27 languages available)

200,000+ machines infected
Spread over 200 countries

Source undetermined

Vulnerability Disclosure: Coordinated

1. Researcher informs vendor about vulnerability and impact
- Usually through a form of report with estimation of impact and/or demonstration

2. Vendor implements and distributes a correction
- But not always!

3. Vulnerability is mostly fixed in supported systems

Optional: CVE entry is requested: https://cveform.mitre.org/

Optional: A website with a sound name is created for public awareness
- Heartbleed, Shellshock, CRIME, POODLE, SPECTRE, LOG4SHELL , BAD NEIGHBOR, Dirty COW…

CVE-2020-15802 – Sep 9 2020

https://hexhive.epfl.ch/BLURtooth/

Researcher:

- "We discovered the vulnerability in March 2020 and responsibly disclosed our findings along with suggested countermeasures to the Bluetooth SIG in May 2020. We kept our findings private and the Bluetooth SIG publicly disclosed them, without informing us, on the 10th of September of 2020. Our work is assigned CVE-2020-15802."

Bluetooth SIG:

- At the time of writing, there are no deployed patches to address the BLUR attacks on actual devices. The Bluetooth SIG suggested that version 5.1 of the standard will contain guidelines to mitigate the BLUR attacks (e.g., disable key overwrites in certain circumstances as proposed in our countermeasures), but such guidelines are not (yet) public and we cannot comment on them. The Bluetooth SIG provides a public statement about BLURtooth and the BLUR attacks.

Vulnerability Disclosure: Full

Researcher discloses the vulnerability without warning

- As a CVE
- In a public mailing list
- As a blog entry, webpage or news item
- As an exploit

Vendor is pressured to issue a fix as soon as possible

- But not always
  - It doesn’t!
  - It considers the product not supported
  - It under reports the issue

Some mayhem may occur until a fix is applied

- Remember all those phones/TVs/etc… without frequent updates

How to disclose

CSIRT Teams define a formal document for the organization

- Follows RFC 2350
- https://www.ua.pt/pt/ciberseguranca/rfc2350
- Contains information about relevant networks, responsible person and contact points
- Signed with PGP

/security.txt defines a formal document for the domain

- Follows RFC 9116
- Machine-parsable format describing their vulnerability disclosure practices to make it easier for researchers to report vulnerabilities

How to disclose

Through the relevant CERT

- https://www.cncs.gov.pt/pt/certpt/
- CERT will inform the target organization directly

https://www.openbugbounty.org/

- Non-profit platform connecting security researchers and domain owners
- Doesn’t imply a payout, but it allows a negotiation

Through contact addresses made available by the entities