IT5504 Information Security 1

Assignment 1

Andrew Graff
2231290

Contents

Introduction

Kia Ora,

What is information security? "Information security is a set of policies, procedures, and principles for safeguarding digital data and other kinds of information" (Yasar, 2023).

It involves the protection of not only our information systems but the processing, storing, and transmitting of these systems through various ways of access. A practice of securing, preventing and how information is shared. It is a constant battle of minimising risks of any intrusion or loss etc regularly by careful implementations of safe security guards and the assurance of measuring these risks.

Information security is everywhere.

In this report, there will be three parts covering three different areas of Information Security. The first part we will be looking into is CIA Triad Definitions. A brief explanation for what CIA stands for (Confidentiality, Integrity, and Availability). These three main concepts branch from the CIA Triad model and is significant in the role it plays in our security systems. We will discuss what each area is and what it means for information security.

Part two of this report is a discussion and evaluation between the New Zealand Cert Personal Security guide and sharing comparison to another guide relatable to personal computer security. This section will be Personal Security Considerations. These guides are designed for any internet user to better protect yourself whilst being online. There are numerous examples and helpful information around personal security which will lead us to exploring a guide to compare with the NZ Cert guide.

Finally, Part three is threats to Computer Security to wrap up our report. In this section we will provide two examples of a CVE with a CVSS score and define these CVE (Common Vulnerabilities and Exposures) and CVSS (Common Vulnerability Scoring System). We will discuss the relationship between CIA Triad and CVSS and conclude this with two examples of CVE with a CVSS from the base metric highlighting CIA Triad impact scores.

Part One: CIA Triad Definitions:

What is CIA Triad? As we discussed in the introduction it stands for Confidentiality, Integrity, and Availability. It is commonly known as a security model used everywhere around the world. A model guided by many Information security policies within organizations.

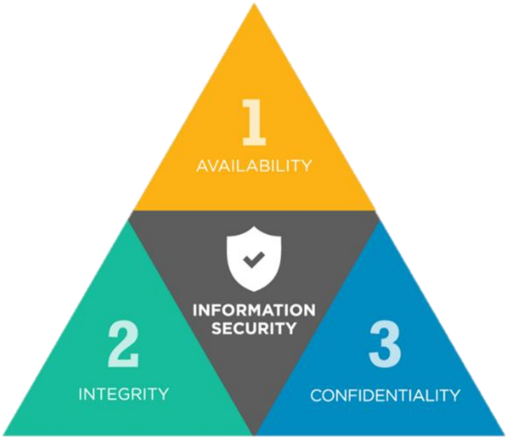


Image: The CIA Triad – Interests and Insights (jamestyson.co.uk)

You will see the CIA is divided into three parts with Information security at the centre and the top being 1. Availability, 2. Integrity and 3. Confidentiality. You would find that these are the three crucial elements of information security and should be at the "forefront of all security decision making within an organisation" (Tyson, 2019). Basically, whenever a company creates or implements a new system, following this CIA Triad model would help alleviate a lot of risks by meeting one or all these elements. Your system will be better secured and covering these three bases would minimise risks or harm to the company, policy, and procedures.

The top of the image we will start with is **Availability.**

Availability means every aspect of the word. In the CIA triad, Availability is where the data and information can be easily accessed by authorised users. This is where systems are up and running and processes can continue, even in the face of an attack. "Without access to our data, everything grinds to a halt, which is why medical and educational institutions like WashU are often targeted for ransomware attacks" (Washington University in St Louis, 2023).

Using applications and accessing our bank account whenever you log in is one of many examples of availability. The accessibility to your personal information via mobile applications at any time reflects this component.

A situation of availability is where I have visited a bank to deposit money to discover the bank had closed. Fortunately, I was able to access the banking mobile application with the ability to transfer between accounts. All accounts are visible and available at my fingertips which reinforces availability.

The second part of this CIA Triad model is Integrity. **What is Integrity?**

Integrity in terms of the CIA triad model and security concept is “data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously” (Fruhlinger, 2020).

By enforcing data integrity, it also protects confidentiality which is what we will discuss more about in our third and final part of the CIA Triad. Integrity or data integrity is provided for example when you are shopping online, and you pay for your items. Your account information will indicate your confirmed purchases via the website with an online emailed receipt. You may have discovered a charge for an item you did not select so this has been reversed based on the data information online. This is data integrity.

I have encountered situations where data integrity has been applied when using our local voting system. This is where the integrity of ballot is designed to prevent election fraud. I would be verified by name and matched in the voting registrar as my vote will be collected independently and sealed for counting by election representatives. “This shows the data can be trusted and maintained in a correct state so it may not be tampered with, and should be correct, authentic, and reliable” (Fasulo, 2021).

The last and final part of our CIA triad model is **Confidentiality.**

“Confidentiality is concerned with preventing unauthorized access to sensitive information. The access could be intentional, such as an intruder breaking into the network and reading the information, or it could be unintentional, due to the carelessness or competence of individuals handling the information” (Brooks, 2019).

This means confidentiality in the concept of security is keeping an organizations data private so that only authorized users and processes should be able to access or modify that data.

A common example of confidentiality can be found in various control methods such as the two-factor authentication, Face ID verification and other access controls. Accessing your medical records online, being prompted to enter a password and inputting a code that has been texted to your mobile device. It is also about letting authorized users in but keeping certain files inaccessible such as seeing your own health history only and no one else’s. Two factor authentication helps keep information secure from accidental disclosure and malicious attacks. Confidentiality is also used when protected data by way of encryption for example using a credit card to make an online purchase. The credit card number is encrypted so that only the intended recipient can read the data.

Personally, I have come across this principle of the CIA triad many times. An important aspect of confidentiality for me is when it is applied when accessing cryptocurrency through my Binance application. There are three layers of security also known as MFA (multi-factor authentication). This access control method involves entering a password, inputting the code sent via text and entering a code generated by the Google Authenticator application. This final principle of the CIA triad ensures my important account information is protected and accessible to me and myself only.

Part Two: Personal Security Considerations

Personal Security is what I would call a prerequisite for any computer user before venturing off on the internet of its world of wonder and the unknowns. The internet can both be a safe and dangerous place if a user has no basic security knowledge that may potentially leave them vulnerable and susceptible to malicious attacks. The simple skillset to identify a website/platform or a person of its authenticity, as well as self-awareness around what information you are sharing, where it is being stored and how it is being secured is certainly something we should take seriously.

We will compare two different personal safety guidelines that helps us with information on being better safe guarded when online are the CERT NZ Personal safety guide and Safety and Cybersecurity Tips, Westpac NZ.

Protect yourself from cybercrime in New Zealand - tips and advice | Westpac NZ

A personal safety guideline we will discuss first is Cybersecurity Tips, Westpac New Zealand "Learn about cybercrime and how to keep your computer and devices safe" 2023 last updated.

Although a New Zealand bank website (Westpac) is of the private sector it has an entire category dedicated to Safety and security online with sub-categories as per the section we will tune in "Cybersecurity tips".

The target audience is primarily those who use online banking but extends to any person who wishes to learn about cybercrime on keeping your computer and devices safe. The language is simple and easy for anyone to read and understand. The group is aimed at banking customers who use everyday banking online and towards the public who need online security tips. We have looked and investigated three principles of the CIA triad model and so we now see which of the three principles match closely to any two of the Cybersecurity tips provided to us by Westpac New Zealand.

The first item on the guide I will recommend based on the CIA triad and the principle would be "Protect your computer and devices with security measures".

In this section, it explains about using other computer or devices and to enable two factor authentication amongst other key tips of not storing passwords or password managers on a shared computer. This most accurately relates to Confidentiality by preventing any unauthorized user from accessing sensitive information, in this case banking account information.

The second item from the Cybersecurity tips would be "Data breaches – Set up security alerts on Westpac One to keep track of online activity". This closely marries against the Integrity principle of the CIA triad model. We have been explained how data integrity is about "data are trustworthy, complete, and have not been accidentally altered or modified by an unauthorised user" (Washington University in St Louis, 2023).

The ability to set up security alerts helps keep track of online activity that will ensure the user is being instantly notified of any unusual activities. This is the bank's promise to ensure the customer is well informed thus falling in accordance with data integrity. The different variations of alerts can be when a balance has exceeded a set amount, or an unknown change of information for example a customer ID has been registered or deregistered from a new/unknown device (mobile, tablet etc). Keeping data up-to date and accurate via these methods is a complete reflection of the Integrity principle of the CIA triad model.

I have explored the Cert NZ which is the top listing when typing in Cyber Security New Zealand. It is also the main website for your first port of call when you need to report a cyber security problem. Analysing this website shows a clearly well listed number of practical tips to keep personal information safe and secure online. There is a downloadable visual poster displaying these practical tips which adds value to those who are not word friendly and can be conveniently printed out and displayed in an office, home or close to where a computer and internet access is nearby.

A guide recommended for a student taking a level 5 course at Whitirea and Weltec who are not in this course would be the NZ Cert. Although, the Cybersecurity tips from the Westpac website is user friendly and easy to read, I would still suggest CERT NZ be the recommended guide. The Westpac cybersecurity guide in this report has hyperlinks to CERT NZ which magnifies my reasons for suggestion.

Part Three: Threats to Computer Security

“Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest” (Garg, 2022).

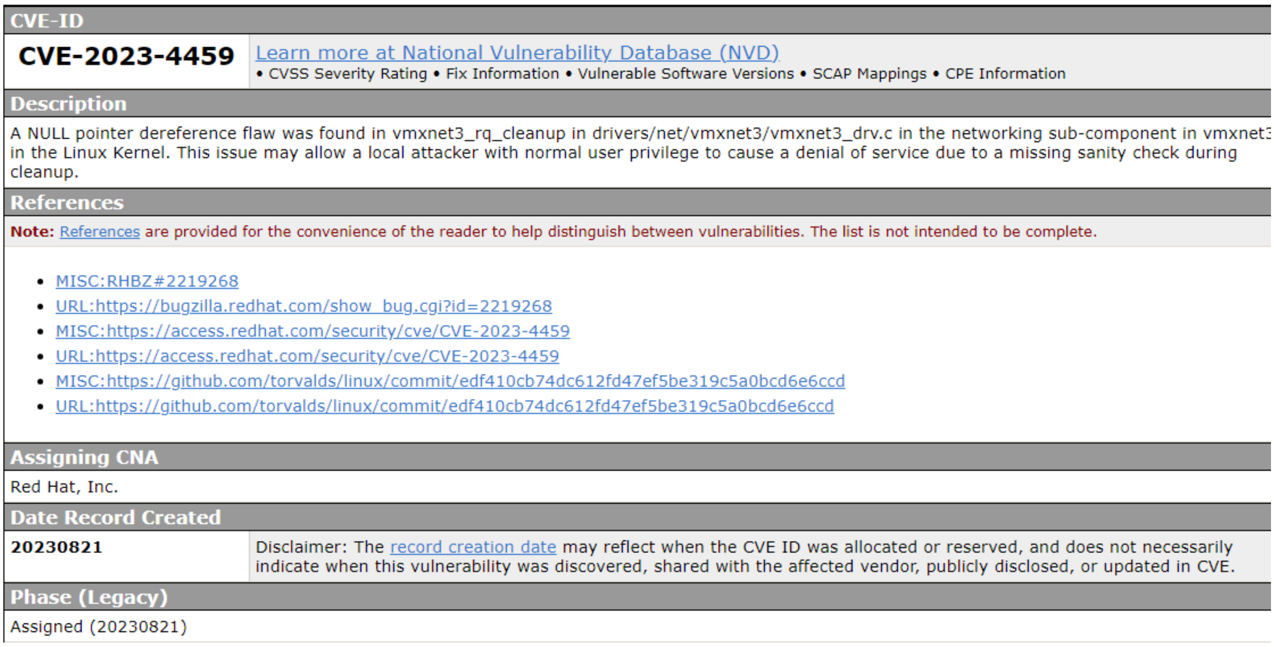
What is CVE and CVSS?

“Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed information security vulnerabilities and exposures” (Tunggal, 2023). What CVE does, it holds reported records of information vulnerability and exposures for organizations to improve their cyber security. It is also a standard that is followed by all vendors such as Microsoft, McAfee security software organisations.

CVE acts as a central repository holding records of all vulnerabilities found in software and hardware components. A standardize identifier also known as CVE names or numbers is created for a vulnerability or exposure. This helps security teams access information about cyber threats under the identifier, providing the public the ability to identify and track vulnerabilities across different systems and platforms.

Using the CVE search bar and typing in “Linux” for example you may find any vulnerabilities of the platform as shown below. The unique CVE identifier is CVE-2023-4459. Which is the year of vulnerability report followed by the next four numbers generated by CNA (CVE Numbering Authority). This is standardized information, meaning it is open for anyone, adding transparency and confidence for both the private and public sector.

Below is an example of a CVE report via Mitre.org



CVE-ID

CVE-2023-4459 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A NULL pointer dereference flaw was found in vmxnet3_rq_cleanup in drivers/net/vmxnet3/vmxnet3_drv.c in the networking sub-component in vmxnet3 in the Linux Kernel. This issue may allow a local attacker with normal user privilege to cause a denial of service due to a missing sanity check during cleanup.

References

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

- MISC:RHBZ#2219268
- URL:https://bugzilla.redhat.com/show_bug.cgi?id=2219268
- MISC:https://access.redhat.com/security/cve/CVE-2023-4459
- URL:https://access.redhat.com/security/cve/CVE-2023-4459
- MISC:https://github.com/torvalds/linux/commit/edf410cb74dc612fd47ef5be319c5a0bcd6e6ccd
- URL:https://github.com/torvalds/linux/commit/edf410cb74dc612fd47ef5be319c5a0bcd6e6ccd

Assigning CNA

Red Hat, Inc.

Date Record Created

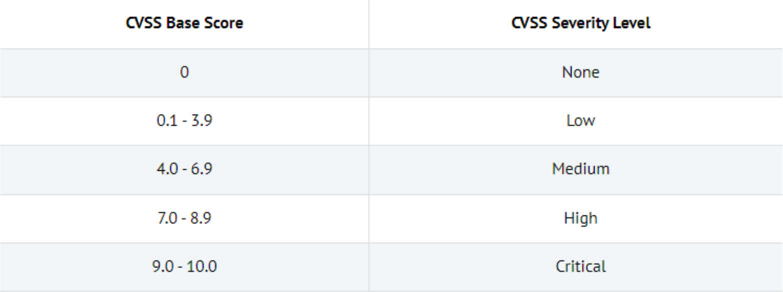
20230821 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20230821)

Image: CVE - CVE-2023-4459 (mitre.org)

"The Common Vulnerabilities Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of software and hardware security vulnerabilities. Its quantitative model aims to ensure consistent and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores" (Murray, 2020).



CVSS Base Score	CVSS Severity Level
0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

Image: What is CVSS - Common Vulnerability Scoring System (sans.org)

The most recent framework of CVSS is CVSS v3.1. The CVSS v3.1 measures severity, not risk and provides a more accurate impact. There are three metric groups the CVSS score consists of: Base, Temporal and Environment. "The base group represents the intrinsic qualities of a vulnerability that are consistent over time and across user environments. The Temporal group reflects the characteristics of a vulnerability that change over time and the environmental group represents a vulnerability unique to a user's environment" (F5,Inc., 2020).

The numeric score produced is an indication of the severity taking various factors into account of vulnerability, exploitability, scope, and impact. These metric groups have an influence on the overall base score.

These are: **AV – Attack vector, AC – Attack complexity, PR – Privileges required, UI - User Interaction, S – Scope, C – Confidentiality, I – Integrity impact and A – Availability impact (CIA Triad).**

CVE and CVSS is one aspect of a holistic bird's eye view of risk management. Taking a broader view allows you to determine what's important and what isn't. These two tools are essential for understanding and addressing software vulnerabilities.

We can see the relationship between CIA Triad & CVSS. As CVSS being the governing body of the overall base score via v3.1, taking in to account the three principles of the CIA triad model.

- **Confidentiality:** Only authorized parties can access the data.
- **Integrity:** Data cannot be modified without authorization.
- **Availability:** Authorized parties can access data when they need to.

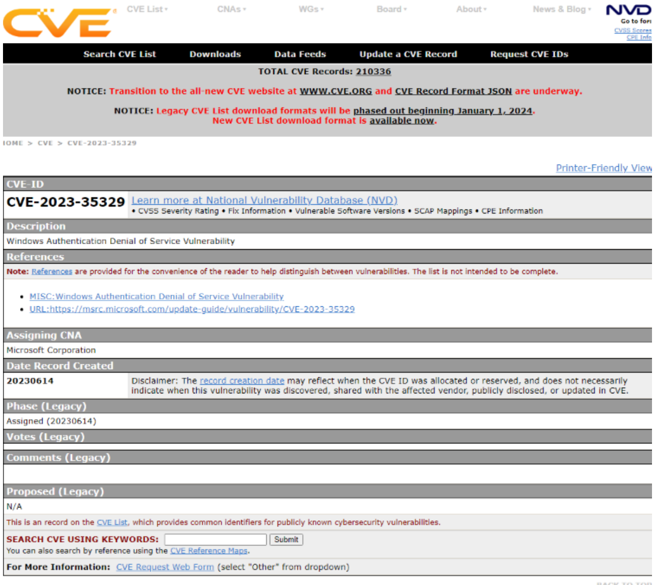
In the next few pages, we will see examples of CVE with a CVSS Score. One is at medium risk which does not require urgent attention however we can see the vulnerability. Another at high risk exploiting vulnerabilities and exposure that needs urgent attention such as patching (fixing the exploit/vulnerability). As a standardized process we can all see this information which proves helpful for everyone.

Two examples of a CVE with a CVSS score

1. CVE-2023-35329

Source: ***Microsoft Corporation***

Windows Authentication Denial of Service Vulnerability.



CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 210336

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

IOME > CVE > CVE-2023-35329

Printer-Friendly View

CVE-ID

CVE-2023-35329 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Windows Authentication Denial of Service 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.

- MISC:Windows Authentication Denial of Service Vulnerability
- URL:https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35329

Assigning CNA

Microsoft Corporation

Date Record Created

20230614 Disclaimer: The record 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 (20230614)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

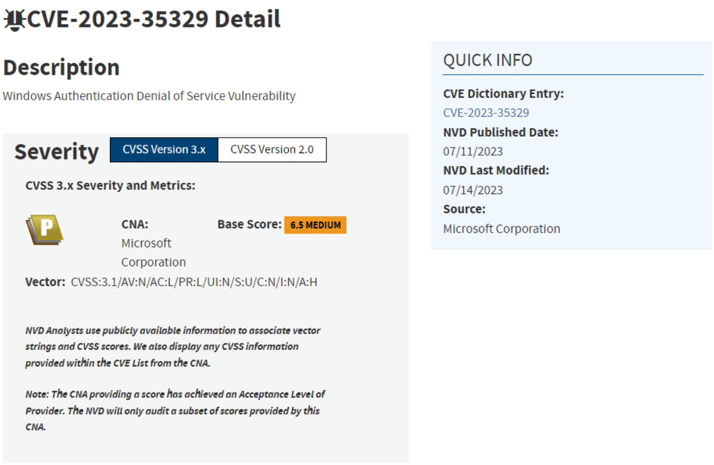
N/A

This is an record 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)

Image: CVE - CVE-2023-35329 (mitre.org)



CVE-2023-35329 Detail

Description

Windows Authentication Denial of Service Vulnerability

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

CNA: Microsoft Corporation **Base Score:** 6.5 MEDIUM

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/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: The CNA providing a score has achieved an Acceptance Level of Provider. The NVD will only audit a subset of scores provided by this CNA.

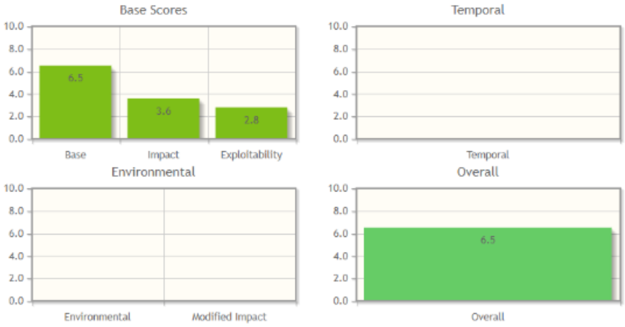
QUICK INFO

CVE Dictionary Entry:
CVE-2023-35329
NVD Published Date:
07/11/2023
NVD Last Modified:
07/14/2023
Source:
Microsoft Corporation

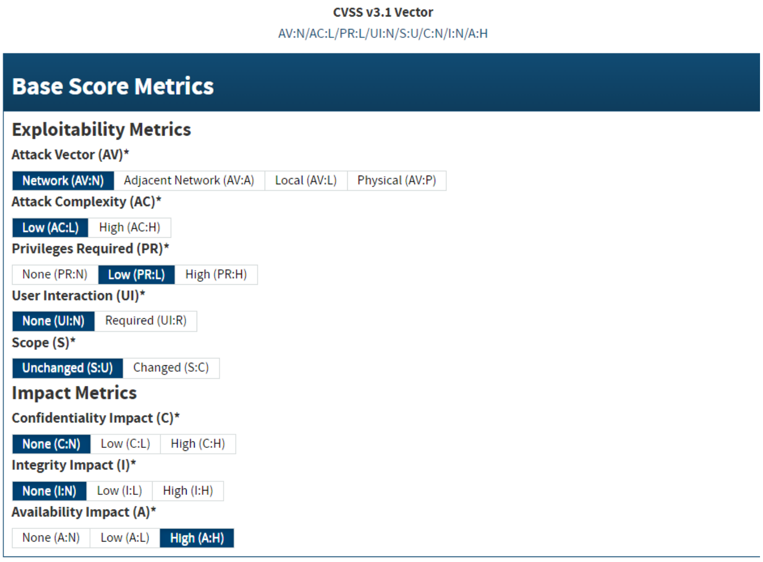
Image: NVD - CVE-2023-35329 (nist.gov)

NIST shows us the **CVE 2023-35329** has a **CVSS V3.1 Base Score** of **6.5 (Medium)**

Below is an expansion of the base score metrics. We can see the CIA triad model as part of the impact metrics scoring. In this example; Confidentiality impact is **none** (not impacted), Integrity impact is **none** and Availability is **high**.



CVSS Base Score: 6.5
Impact Subscore: 3.6
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.5



CVSS v3.1 Vector
AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*
[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*
None (PR:N) [✓ Low (PR:L)] High (PR:H)

User Interaction (UI)*
[✓ None (UI:N)] Required (UI:R)

Scope (S)*
[✓ Unchanged (S:U)] Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
[✓ None (C:N)] Low (C:L) High (C:H)

Integrity Impact (I)*
[✓ None (I:N)] Low (I:L) High (I:H)

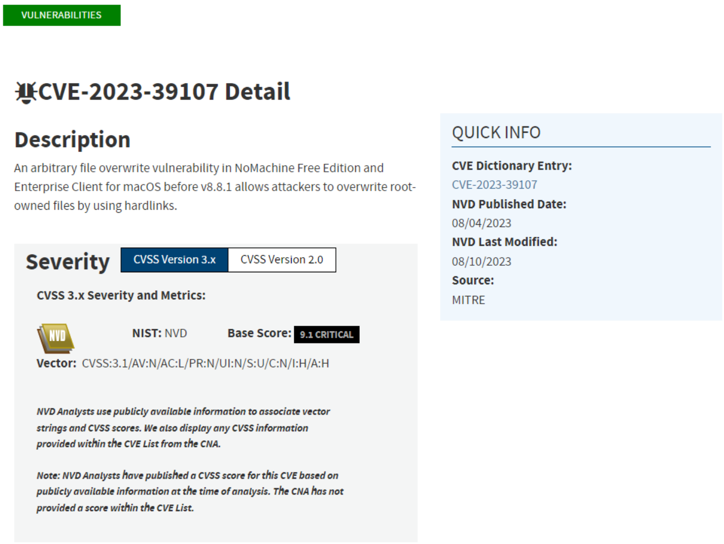
Availability Impact (A)*
None (A:N) Low (A:L) [✓ High (A:H)]

Image: NVD - CVSS v3 Calculator (nist.gov)

2. CVE-2023-39107

Source: ***Mitre***

An arbitrary file overwrite vulnerability in NoMachine Free Edition and Enterprise Client for macOS before v8.8.1 allows attackers to overwrite root-owned files by using hardlinks.



VULNERABILITIES

CVE-2023-39107 Detail

Description

An arbitrary file overwrite vulnerability in NoMachine Free Edition and Enterprise Client for macOS before v8.8.1 allows attackers to overwrite root-owned files by using hardlinks.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.1 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/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.

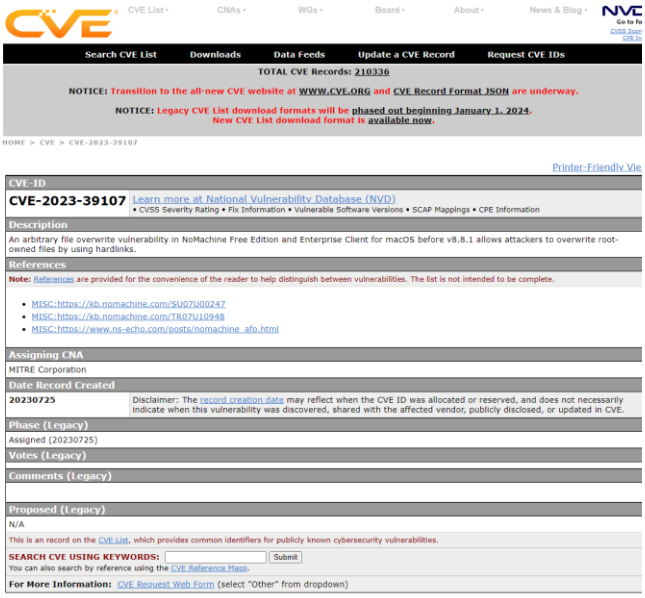
Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2023-39107
NVD Published Date:
08/04/2023
NVD Last Modified:
08/10/2023
Source:
MITRE

Image: NVD - CVE-2023-39107 (nist.gov)

NIST shows us the **CVE 2023-39107** has a **CVSS v3.1 Base Score** of **9.1 (Critical)**



TOTAL CVE Records: 210336

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > CVE-2023-39107

Printer-Friendly Vie

CVE-ID

CVE-2023-39107 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An arbitrary file overwrite vulnerability in NoMachine Free Edition and Enterprise Client for macOS before v8.8.1 allows attackers to overwrite root-owned files by using hardlinks.

References

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

- MISC:https://kb.nomachine.com/SU07U00247
- MISC:https://kb.nomachine.com/TR07U10948
- MISC:https://www.ns-echo.com/posts/nomachine_afo.html

Assigning CNA

MITRE Corporation

Date Record Created

20230725 Disclaimer: The record 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 (20230725)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

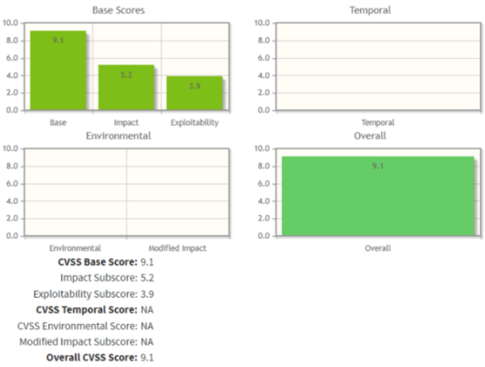
This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

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

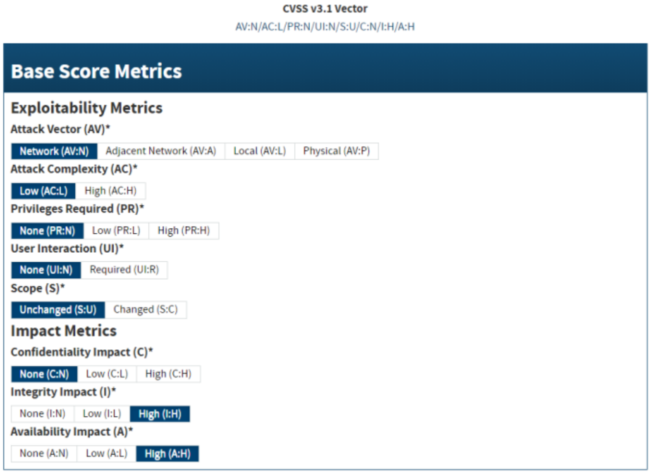
For More Information: CVE Request Web Form (select "Other" from dropdown)

Image: CVE - CVE-2023-39107 (mitre.org)

Below is an expansion of the base score metrics. We can see the CIA triad model as part of the impact metrics scoring. In this example; Confidentiality impact is **none** (not impacted), Integrity impact is **high** and Availability is **high**.



CVSS Base Score: 9.1
Impact Subscore: 5.2
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 9.1



CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

Image: NVD - CVSS v3 Calculator (nist.gov)

Referencing

(Brooks, 2019)	Brooks, R. (2019, Mar 26). *What is the CIA triad?* Confidentiality. The CIA Triad and Real-World Examples (netwrix.com)
(Fasulo, 2021)	Fasulo, P. (2021, Jan 9). *Why is the CIA triad important?* Integrity. What is the CIA Triad? Definition, Importance, & Examples | SecurityScorecard
(Fruhlinger, 2020)	Fruhlinger, J. (2020, Feb 10). *The CIA triad: Definition components and examples.* Integrity. The CIA triad: Definition, components and examples | CSO Online
(F5,Inc., 2020)	[F5,Inc.]. (2020, March 4). *What is Common Vulnerability Scoring System (CVSS)* [Video]. YouTube. What is Common Vulnerability Scoring System (CVSS) - YouTube
(Garg, 2022)	Garg, R. (2022, Jun 28). *Threats to Information Security.* Threats to Information Security - GeeksforGeeks
(Murray, 2020)	Murray, A. (2020, Nov 14). *What is CVSS v3.1? Understanding The New CVSS.* What Is CVSS v3.1? Understanding The New CVSS | Mend
(Risto, 2023)	Risto, J. (2023, May 22). *What is CVSS? Common Vulnerability Scoring System (CVSS).* What is CVSS - Common Vulnerability Scoring System (sans.org)
(Tunggal, 2023)	Tunggal, A. (2023, Apr 06). *What is CVE? Common Vulnerabilities and Exposures Explained.* What is a CVE? Common Vulnerabilities and Exposures Explained | UpGuard
(Tyson, 2019)	Tyson, J. (2019, March 30). *The CIA Triad.* Interests and Insights. The CIA Triad – Interests and Insights (jamestyson.co.uk)
(Washington University in St. Louis, 2023)	Washington University in St Louis. (2023).

	Office of Information Security. Availability. Availability | Office of Information Security | Washington University in St. Louis (wustl.edu)
(Washington University in St. Louis, 2023)	Washington University in St Louis. (2023). *Office of Information Security.* Integrity. Integrity | Office of Information Security | Washington University in St. Louis (wustl.edu)
(Yasar, 2023)	Yasar, K. (2000-2023). *What is information security?*. Tech Target. What is Information Security (Infosec)? – TechTarget Definition