



## Official incident report

Event ID: 229

Rule Name: SOC262 - ScreenConnect Authentication Bypass  
Exploitation Detected (CVE-2024-1709)

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: <https://www.linkedin.com/in/ahmed-mansour-5631b5323/>

Github link: <https://github.com/AhmedMansour93>

# Table of contents

<b>Official incident report</b>	<b>1</b>
Event ID: 268	1
Rule Name: SOC262 - ScreenConnect Authentication Bypass Exploitation Detected (CVE-2024-1709)	1
<b>Table of contents</b>	<b>2</b>
<b>Event Details</b>	<b>3</b>
<b>Network Information Details</b>	<b>4</b>
<b>Analysis</b>	<b>5</b>
Log management	5
<b>Security Email</b>	<b>8</b>
<b>Detection</b>	<b>9</b>
Threat intelligence	9
<b>Endpoint Security</b>	<b>10</b>
<b>Conclusion</b>	<b>11</b>

# Event Details

**Event ID:**

229

**Event Date and Time:**

Feb, 22, 2024, 01:39 AM

**Rule:**

SOC262 - ScreenConnect Authentication Bypass Exploitation Detected (CVE-2024-1709)

**Level:**

Incident Responder

**Hostname:**

ScreenConnect Server 23.9.7

**HTTP Request Method:**

GET

**Requested URL:**

172.16.17.65/SetupWizard.aspx/

**Alert Trigger Reason:**

'/SetupWizard.aspx/' Detected on Get Request, indicative of exploitation of the ScreenConnect vulnerability CVE-2024-1709.

**L1 Note:**

The host is a Windows Server running Remote Desktop and access software named ScreenConnect. Suspicious network traffic associated with the reported zero-day vulnerability has been identified on the device. Escalating to L2 for in-depth analysis and investigation.

# Network Information Details

## Destination IP Address:

172.16.17.65 internal

## Source IP Address:

118.69.65.60 external

- **172.16.17.65 (Internal):**
  - This is an internal IP address associated with a server in your network. IP addresses in the range 172.16.0.0 to 172.31.255.255 are private and used within internal networks. These addresses are not routable on the public internet, meaning they belong to your organization's internal infrastructure.

## Source IP Address:

- **118.69.65.60 (External):**
  - This is a public IP address, indicating that the request originated from outside your organization's internal network. This suggests that the attack or connection attempt came from an external source, likely over the internet.
  - **The attack is external**, coming from an IP address outside of your organization's controlled network.

# Analysis:

## Log Management

We'll proceed by entering the destination IP address and reviewing the results.

Please refer to the attached image for further details regarding the attack.

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Columns	Operator	Value				
X Dest. Address	contains	172.16.17.65				
Feb, 22, 2024, 01:28 PM	Firewall	118.69.65.60	60520	172.16.17.65	8040	
Feb, 22, 2024, 01:31 PM	Firewall	118.69.65.60	15382	172.16.17.65	8040	
Feb, 22, 2024, 01:39 PM	Firewall	118.69.65.60	19902	172.16.17.65	8040	

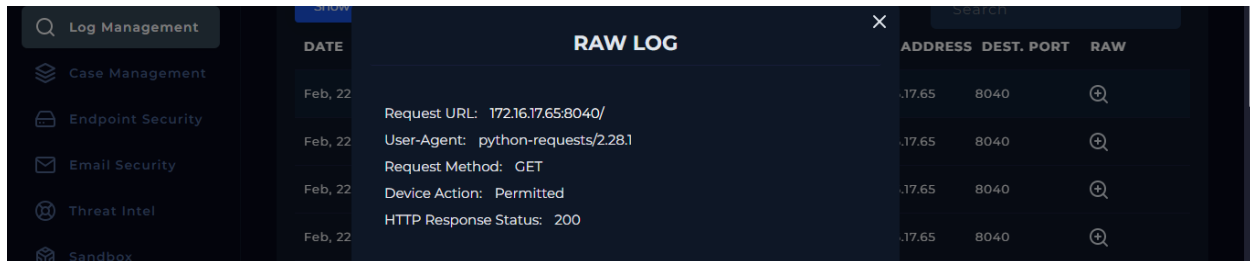
### 4 Logs records for the destination IP.

Please refer to the attached image for further details regarding the attack.

We will explain all of them step by step

## Log Analysis

- **Log1:**

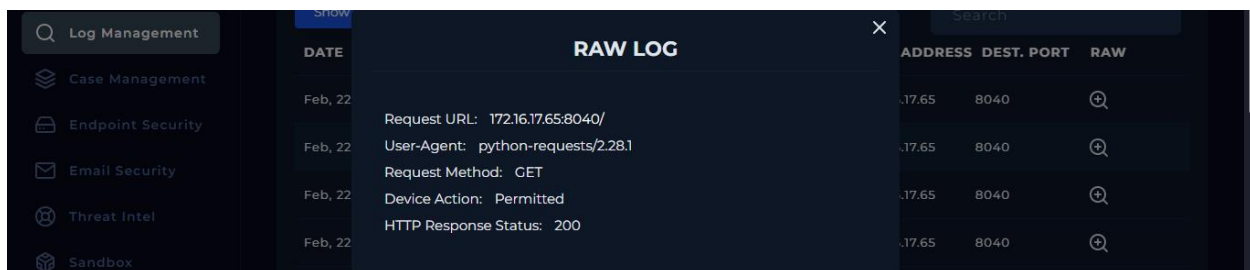


DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
Feb, 22	Request URL: 172.16.17.65:8040/	172.16.17.65	8040	[icon]
Feb, 22	User-Agent: python-requests/2.28.1	172.16.17.65	8040	[icon]
Feb, 22	Request Method: GET	172.16.17.65	8040	[icon]
Feb, 22	Device Action: Permitted	172.16.17.65	8040	[icon]
Feb, 22	HTTP Response Status: 200	172.16.17.65	8040	[icon]

### What Happened:

In this log, the Python script made a successful request to the root directory of the web server hosted at 172.16.17.65:8040. The server responded with a 200 status code, meaning the requested resource was available, and no security controls blocked the request.

- **Log2:**

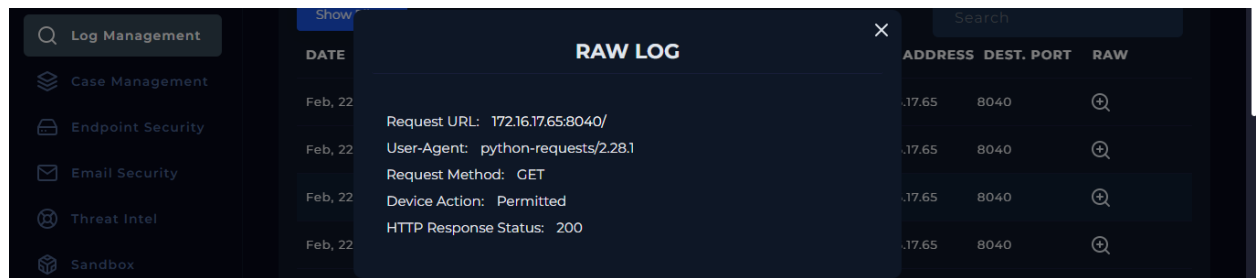


DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
Feb, 22	Request URL: 172.16.17.65:8040/	172.16.17.65	8040	[icon]
Feb, 22	User-Agent: python-requests/2.28.1	172.16.17.65	8040	[icon]
Feb, 22	Request Method: GET	172.16.17.65	8040	[icon]
Feb, 22	Device Action: Permitted	172.16.17.65	8040	[icon]
Feb, 22	HTTP Response Status: 200	172.16.17.65	8040	[icon]

### What Happened:

This log shows another successful GET request to the same URL as in Log 1. The Python script was able to retrieve the resource from the web server again, with no issues reported.

- **Log3:**



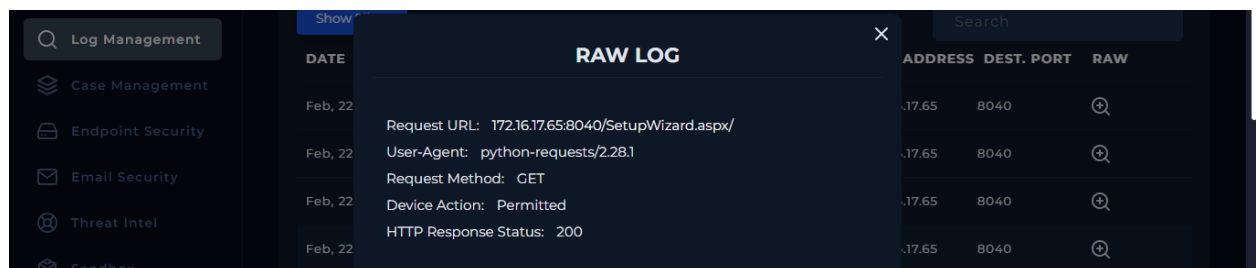
The screenshot shows a 'Log Management' sidebar on the left with options: Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area displays a 'RAW LOG' window with a search bar and a table of logs. The table has columns: DATE, ADDRESS, DEST. PORT, and RAW. The logs show a sequence of requests from 172.16.17.65 to port 8040, including a GET request for the root URL and a permitted device action.

DATE	ADDRESS	DEST. PORT	RAW
Feb, 22	172.16.17.65	8040	Request URL: 172.16.17.65:8040/
Feb, 22	172.16.17.65	8040	User-Agent: python-requests/2.28.1
Feb, 22	172.16.17.65	8040	Request Method: GET
Feb, 22	172.16.17.65	8040	Device Action: Permitted
Feb, 22	172.16.17.65	8040	HTTP Response Status: 200

## What Happened:

This log repeats the pattern of successful requests to the root URL. The Python script is continuously able to access the server's root directory without any issues, suggesting normal behavior at this stage.

- **Log4:**



The screenshot shows the same 'Log Management' interface as Log3, but with a different log entry selected. The 'RAW LOG' window now shows a GET request for the SetupWizard.aspx page, which is used for configuring or initializing the web service.

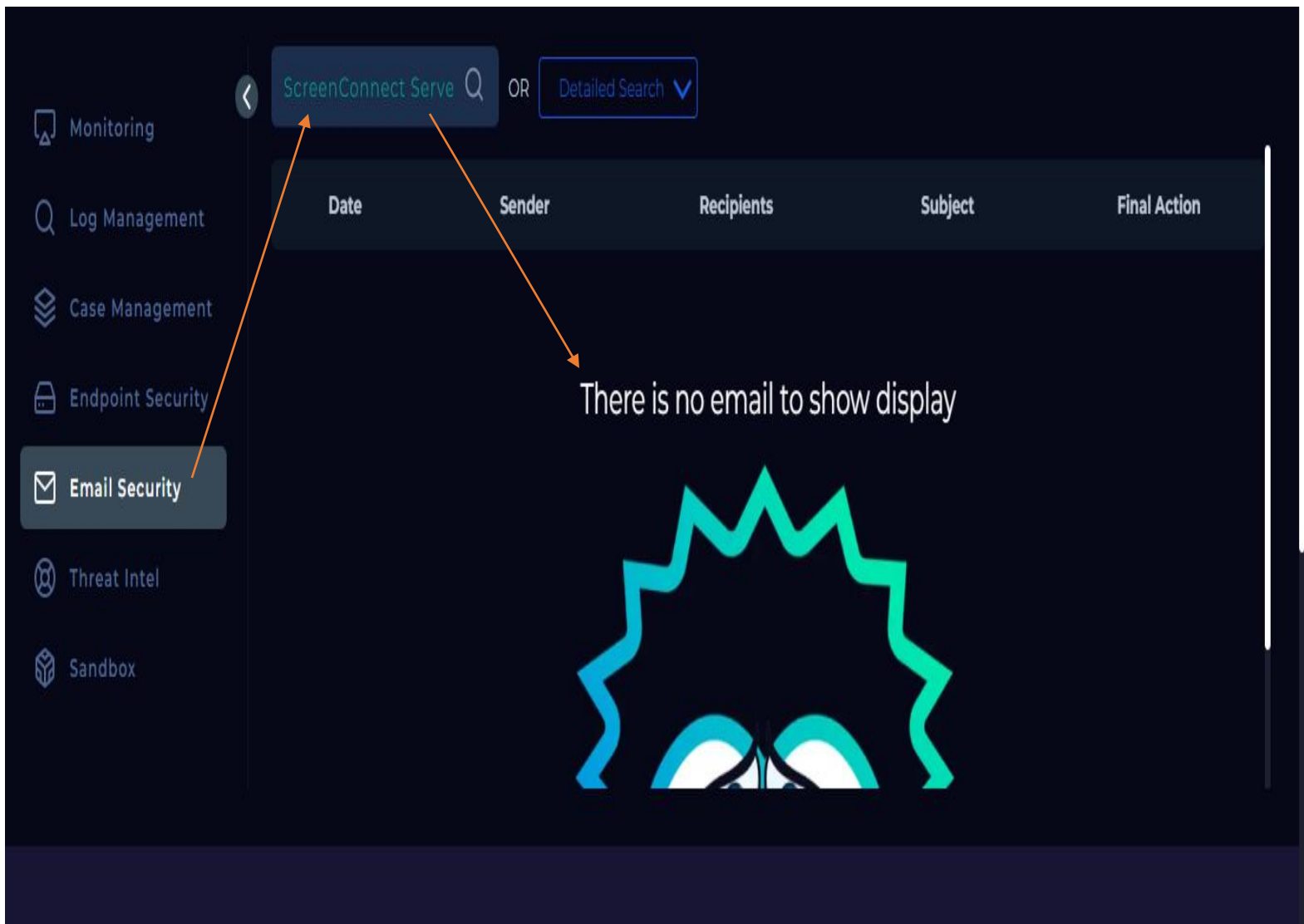
DATE	ADDRESS	DEST. PORT	RAW
Feb, 22	172.16.17.65	8040	Request URL: 172.16.17.65:8040/SetupWizard.aspx/
Feb, 22	172.16.17.65	8040	User-Agent: python-requests/2.28.1
Feb, 22	172.16.17.65	8040	Request Method: GET
Feb, 22	172.16.17.65	8040	Device Action: Permitted
Feb, 22	172.16.17.65	8040	HTTP Response Status: 200

## What Happened:

In this log, the Python script successfully accessed the SetupWizard.aspx page, which is likely used for configuring or initializing the web service. This could be part of a legitimate setup process, or it could indicate a potential attempt to exploit an exposed configuration page.

- **The Attack Were Successful.**

## Email Security:



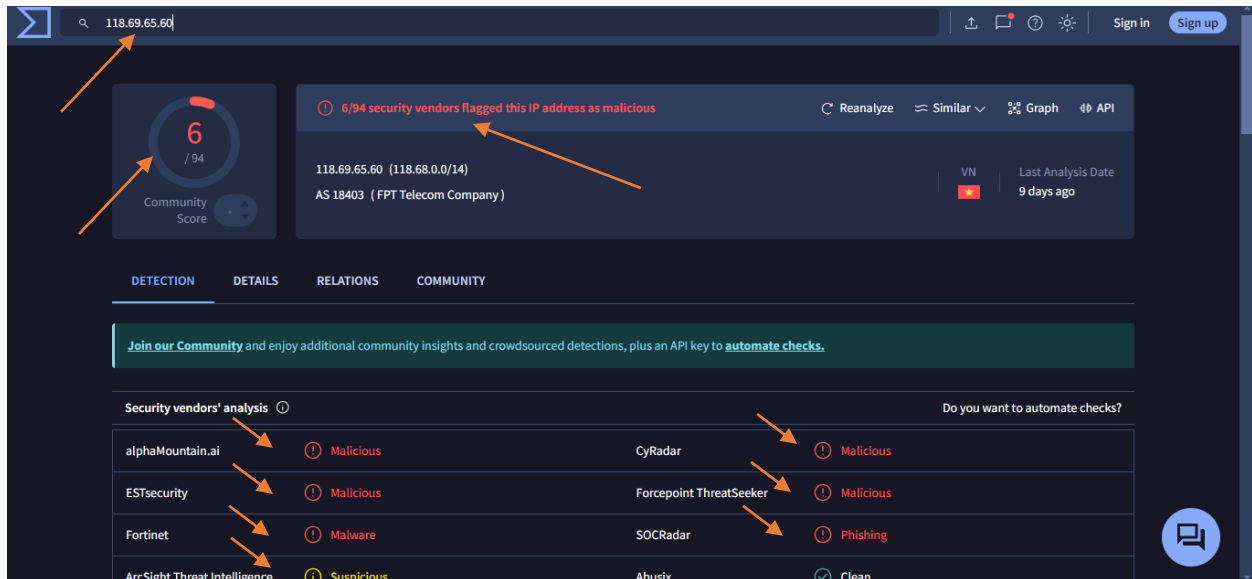
- **Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed.**



## Detection:

## Threat Intelligence Results

We will conduct a comprehensive scan of the source IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



## Analysis Results:

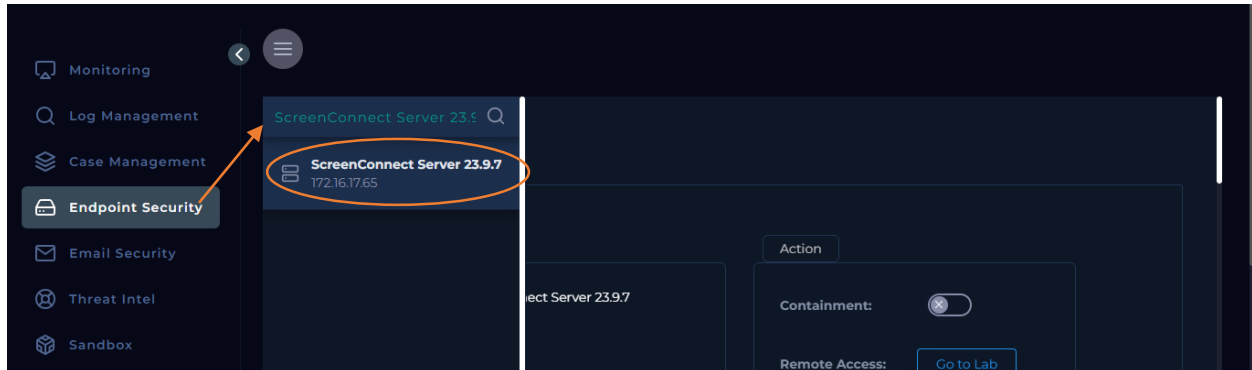
Out of 94 security vendors, 6 have flagged the IP address **118.69.65.60** as malicious. Below is a breakdown of the vendors and their respective threat classifications:

- **alphaMountain.ai:** Malicious
- **CyRadar:** Malicious
- **ESTsecurity:** Malicious
- **Forcepoint ThreatSeeker:** Malicious
- **Fortinet:** Malware
- **SOCRadar:** Phishing

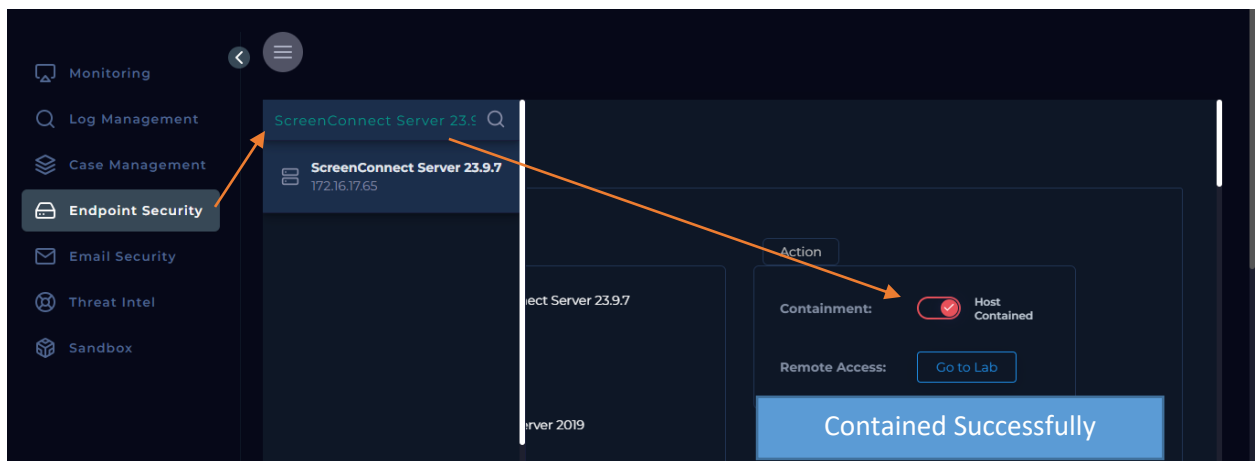
These results indicate a strong likelihood of malicious activity originating from this IP address, including malware distribution and phishing attempts

- [Reference result.](#)
- **The Traffic is Malicious**

## Endpoint Security:



- Based on our analysis, the reconnaissance activity identified is focused on gathering victim and company user's identity information's.
- The device must be Contain. And we contained Successfully.



# Conclusion:

The incident involving **Event ID 229** on **Feb 22, 2024**, pertains to the detection of an attempted exploitation of **ScreenConnect Authentication Bypass (CVE-2024-1709)**. The suspicious traffic was identified as originating from an external IP address (**118.69.65.60**), targeting the internal server (**172.16.17.65**) hosting the ScreenConnect service.

Upon reviewing the logs, it was observed that the attacker made several **GET** requests using a Python script to the internal server. Notably, the request for the `SetupWizard.aspx` page raised a critical alert, as it indicates potential exploitation of the vulnerable setup process in ScreenConnect.

A comprehensive threat intelligence analysis revealed that the source IP is flagged by multiple security vendors for **malicious activities**, including **malware distribution** and **phishing**. This reinforces the conclusion that the external entity posed a legitimate threat to our infrastructure.

Given the reconnaissance nature of the activity, the primary focus of the attacker appears to have been gathering sensitive user and company information through the exploitation attempt. Fortunately, our response team swiftly acted to **contain the device** and prevent further exploitation.

In summary, the malicious traffic was successfully identified, analyzed, and contained, preventing any further escalation or compromise of internal systems. The timely detection and effective containment demonstrate the robustness of our incident response process in mitigating high-risk threats.