COMPREHENSIVE CYBERSECURITY ANALYSIS REPORT IP 194.169.172.169

PREPARED BY

Patel Vasu

WEDNESDAY, JANUARY 08, 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

THIS REPORT PROVIDES AN IN-DEPTH TECHNICAL EVALUATION OF THE IP ADDRESS **194.169.172.169**, WHICH IS ASSOCIATED WITH SUSPICIOUS ACTIVITY, POOR REPUTATION, AND MULTIPLE ABUSE REPORTS. THE ANALYSIS INCLUDES REPUTATION SCORING, OPEN PORT VULNERABILITIES, SSL DETAILS, ABUSE REPORTS, AND ACTIONABLE RECOMMENDATIONS FOR CYBERSECURITY TEAMS.

SECTION 1: GENERAL IP INFORMATION

IP Address: 194.169.172.169

Hostname: juice.teaori.com

Domain: teaori.com

Network Owner: Neterra Ltd.

Country: Bulgaria

Forward/Reverse DNS Match: No data available

Content Category: Not categorized

SECTION 2: REPUTATION ANALYSIS

Reputation Metrics

- Sender IP Reputation: Poor
- Web Reputation: Unknown
- Spam Level: Critical

Blocklist Status

- Spamhaus SBL: Listed
- SpamCop, CBL, PBL: Not Listed
- Talos Intelligence: Not Listed

SECTION 3: EMAIL ACTIVITY ANALYSIS

Email Volume Data

Daily Email Volume: 0.0 emails

Monthly Email Volume: 4.9 emails

Volume Change: -31.11%

SECTION 4: ABUSE REPORTS

Overview

- Total Reports: 10
- Confidence of Abuse: 30%
- First Report: December 10, 2024
- Most Recent Report: 3 weeks ago

Specific Reports

- Eurofluid: Multiple instances of port scans, hacking attempts, and brute-force attacks.
- Anonymous Reports Include:

1. Brute-force SSH attacks.
2. Phishing email campaigns flagged by spam filters.
3. SMTP scanning attempts (relay access denied).

SECTION 5: NETWORK ANALYSIS

Peer IP Reputation

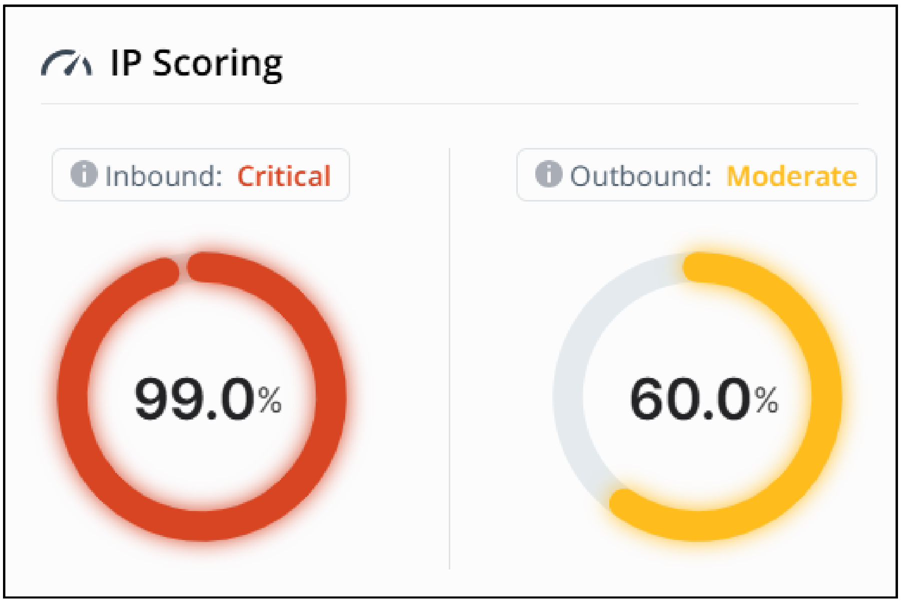
Neighboring IPs show a mix of good and suspicious reputations. The IP address appears within a network block with potential legitimate activity interspersed with anomalous behavior.

SECTION 6: VULNERABILITIES AND OPEN PORTS

Critical Scoring

Inbound Threats: 99.0% likelihood.

Outbound Threats: 60.0% likelihood.



IP Scoring

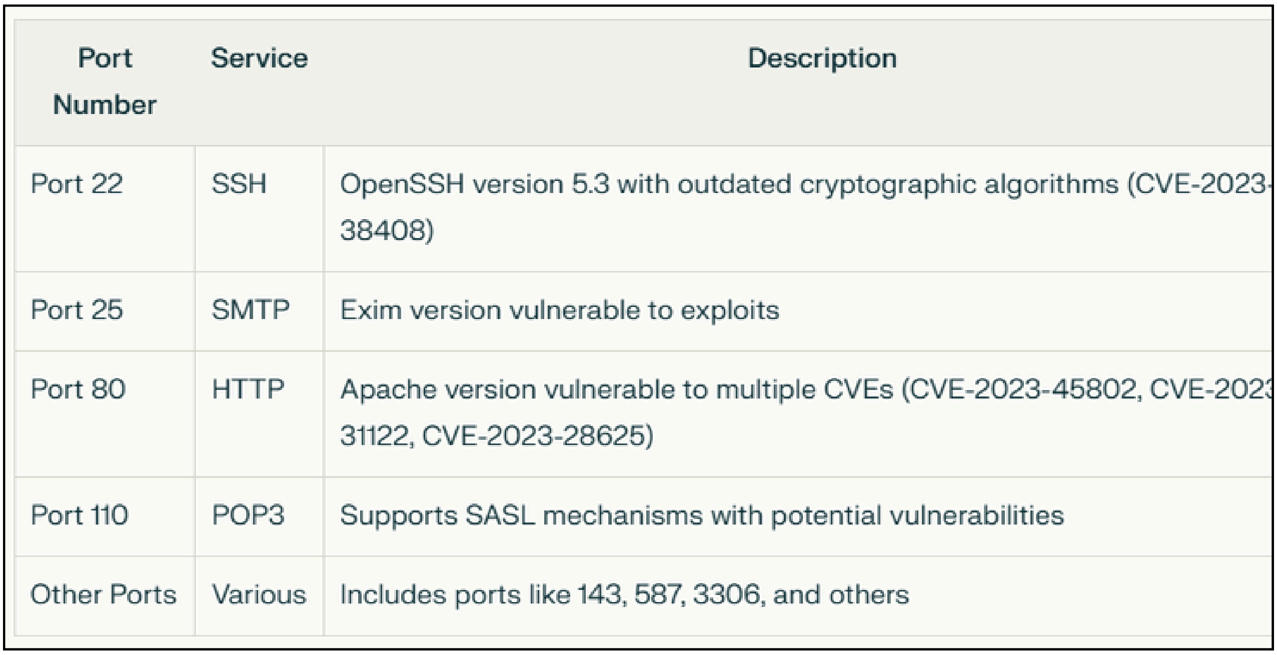
Inbound: Critical

99.0%

Outbound: Moderate

60.0%

Open Ports



Port Number	Service	Description
Port 22	SSH	OpenSSH version 5.3 with outdated cryptographic algorithms (CVE-2023-38408)
Port 25	SMTP	Exim version vulnerable to exploits
Port 80	HTTP	Apache version vulnerable to multiple CVEs (CVE-2023-45802, CVE-2023-31122, CVE-2023-28625)
Port 110	POP3	Supports SASL mechanisms with potential vulnerabilities
Other Ports	Various	Includes ports like 143, 587, 3306, and others

Vulnerabilities Summary

CVE Details:

CVE-2023-45802

CWE: CWE-400 (Uncontrolled Resource Consumption)

Protocol: TCP on Port 80

CVSS v3 Score: Medium

Vendor: Apache

Description: Memory resources not reclaimed immediately when an HTTP/2 stream is reset by a client; can lead to memory exhaustion before connection closure.

Recommendation: Upgrade to Apache version 2.4.58 or later.

CVE-2023-38408

CWE: CWE-20 (Improper Input Validation)

Protocol: TCP on Port 22

CVSS v3 Score: Critical

Vendor: OpenBSD

Description: Insufficiently trustworthy search path in ssh-agent leading to remote code execution if forwarded to an attacker-controlled system.

Recommendation: Upgrade to OpenSSH version 9.3p2 or later.

CVE-2023-31122

CWE: CWE-20 (Improper Input Validation)

Protocol: TCP on Port 80

CVSS v3 Score: High

Vendor: Apache

Description: Out-of-bounds read vulnerability in mod_macro affecting versions up to and including Apache HTTP Server version 2.4.57.

Recommendation: Upgrade to the latest Apache version.

CVE-2023-28625

CWE: CWE-20 (Improper Input Validation)

Protocol: TCP on Port 80

CVSS v3 Score: High

Vendor: Apache

Description: NULL pointer dereference in mod_auth_openidc leading to segmentation fault under certain conditions.

Recommendation: Upgrade to version 2.4.13.2 or later.

SSL Certificate Details

Type: Self-Signed

Validity Period: December 4, 2024 – December 4, 2025

Issuer & Subject: juice.teaori.com (Vesta Control Panel)

SHA256 Fingerprint: 450744c059ce03686db9a72290d012c3a70e50f46f7e8672f05316d10498b15e

SECTION 7: VIRUSTOTAL ANALYSIS

BASIC INFORMATION

IP ADDRESS: 194.169.172.169

ASN: AS215998 (MORTEZA ESKANDARI)

COUNTRY: BULGARIA (BG)

REGIONAL INTERNET REGISTRY: RIPE NCC

COMMUNITY AND VENDOR SCORES

COMMUNITY SCORE: 1/94

SECURITY VENDOR FLAGGING RATE: 1/94 FLAGGED THIS IP AS MALICIOUS

LAST ANALYSIS DATE: JANUARY 2, 2025

DETECTION DETAILS FROM VIRUSTOTAL

PASSIVE DNS REPLICATION:

TEAORI.COM (4/94 DETECTIONS)

JUICE.TEAORI.COM (0/94 DETECTIONS)

JAYPEGAMS.COM (0/94 DETECTIONS)

JAPAN.JAYPEGAMS.COM(0/94 DETECTIONS)

Files Referring to IP Address:

FileName:

estima@favellefavco.com.my_download(1).eml

Detection Rate:

15/62 vendors flagged as malicious

File Name:

localfile~

Detection Rate:

25/63 vendors flagged as malicious

File Name:

717E06940006.36.1718075202.620317.1.eml

Detection Rate:

21/63 vendors flagged as malicious

SECTION 8: RECOMMENDATIONS AND NEXT STEPS

Examine Activity

1. Identify patterns of interaction and irregular behavior through:

- Analyzing authentication logs for failed login attempts.
- Using tools like Zeek or Wireshark for network traffic examination.

Uncover Associations

1. Link the IP to known threat campaigns by:

- Cross-checking threat intelligence databases.

Extract Evidence

1. Collect forensic artifacts such as:

- Logs of communication pathways.
- Payload analyses for malicious scripts.

CONCLUSION

THE IP ADDRESS 194.169.172.169 POSES SIGNIFICANT RISKS DUE TO ITS ASSOCIATION WITH ABUSE REPORTS, VIRUSTOTAL DETECTIONS, AND CRITICAL VULNERABILITIES LIKE THOSE FOUND IN APACHE HTTP SERVER AND OPENSSH SOFTWARE COMPONENTS LISTED ABOVE. IMMEDIATE MITIGATION STRATEGIES AND ONGOING MONITORING ARE RECOMMENDED TO SAFEGUARD AGAINST POTENTIAL THREATS. NOTE: THIS REPORT SHOULD BE REVIEWED REGULARLY FOR UPDATES ON VULNERABILITIES AND REMEDIATION STEPS AS NEW INFORMATION BECOMES AVAILABLE FROM TRUSTED SECURITY SOURCES LIKE TWINGATE, IBM SECURITY BULLETINS, AND CVE DATABASES .