

Security Analysis Report

Comprehensive Security Assessment and Threat Analysis



Vulnerability Analysis

In-depth security assessment with CVSS scoring and detailed remediation guidance



MITRE Coverage

Comprehensive evaluation of security events and MITRE ATT&CK framework alignment

CONTENTS

OVERVIEW

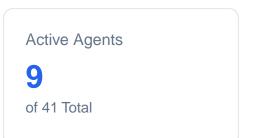
Executive Summary	3
<u>Vulnerability Analysis</u>	4
MITRE ATT&CK Analysis	<u>5</u>

AGENT ANALYSIS

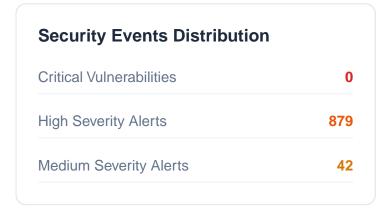
Agent 1 Analysis	<u>6</u>
Agent 2 Analysis	7
Agent 3 Analysis	8
Agent 4 Analysis	9
Agent 5 Analysis	10
Agent 6 Analysis	11
Agent 7 Analysis	12
Agent 8 Analysis	<u>13</u>
Agent 9 Analysis	14

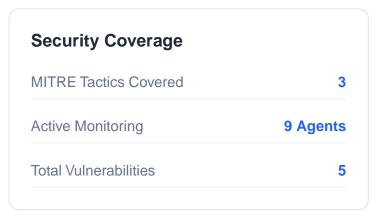
Security assessment across 41 agents reveals a security score of 0 (Critical). The analysis identified 0 critical vulnerabilities and 879 high-severity alerts that require attention. Security monitoring covers 3 MITRE ATT&CK tactics.











Key Recommendations

High Severity Alerts

Review and respond to 879 high severity security events that may indicate significant security threats.

MITRE Coverage

Expand security monitoring to cover more MITRE ATT&CK tactics for comprehensive threat detection.

Detected **5 vulnerabilities** across all agents. This analysis includes CVSS scores, affected packages, and detailed vulnerability information to help prioritize remediation efforts.

0

Critical Vulnerabilities

5

High Severity

0

Medium Severity

Other Vulnerabilities

CVE-2024-6345

High

CVE-2024-6345 affects setuptools

A vulnerability in the package_index module of pypa/setuptools versions up to 69.1.1 allows for remote code execution via its download functions. These functions, which are used to download packages from URLs provided by users or retrieved from package index servers, are susceptible to code injection. If these functions are exposed to user-controlled inputs, such as package URLs, they can execute arbitrary commands on the system. The issue is fixed in version 70.0.

CVSS v3 Score

8.800000

Attack Vector: NETWORK

Availability: HIGH

Confidentiality Impact: HIGH

Integrity Impact: HIGH

Privileges Required: NONE

Scope: UNCHANGED

User Interaction: REQUIRED

Affected Package

setuptools (65.5.0)

Architecture:

Published: July 15, 2024

Updated: July 15, 2024

CVE-2023-36632

High

CVE-2023-36632 affects Python 3.10.10 (64-bit)

The legacy email.utils.parseaddr function in Python through 3.11.4 allows attackers to trigger "RecursionError: maximum recursion depth exceeded while calling a Python object" via a crafted argument. This argument is plausibly an untrusted value from an application's input data that was supposed to contain a name and

an e-mail address. NOTE: email.utils.parseaddr is categorized as a Legacy API in the documentation of the Python email package. Applications should instead use the email.parser.BytesParser or email.parser.Parser class. NOTE: the vendor's perspective is that this is neither a vulnerability nor a bug. The email package is intended to have size limits and to throw an exception when limits are exceeded; they were exceeded by the example demonstration code.



Availability: HIGH Confidentiality Impact: NONE Integrity Impact: NONE Privileges Required: NONE

Scope: UNCHANGED User Interaction: NONE

Affected Package

Python 3.10.10 (64-bit) (3.10.10150.0)

Architecture:

Published: June 26, 2023 Updated: August 3, 2024

CVE-2023-24329 High

CVE-2023-24329 affects Python 3.10.10 (64-bit)

An issue in the urllib.parse component of Python before 3.11.4 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters.

CVSS v3 Score

7.500000

Availability: NONE Confidentiality Impact: NONE Integrity Impact: HIGH Privileges Required: NONE

Scope: UNCHANGED User Interaction: NONE

Affected Package

Python 3.10.10 (64-bit) (3.10.10150.0)

Architecture:

Published: February 17, 2023 Updated: November 7, 2023

CVE-2024-7592 High

CVE-2024-7592 affects Python 3.10.10 (64-bit)

There is a LOW severity vulnerability affecting CPython, specifically the 'http.cookies' standard library module. When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value.

CVSS v3 Score

7.500000

Availability: HIGH Confidentiality Impact: NONE Integrity Impact: NONE Privileges Required: NONE

Scope: UNCHANGED User Interaction: NONE

Affected Package

Python 3.10.10 (64-bit) (3.10.10150.0)

Architecture:

Published: August 20, 2024 Updated: September 5, 2024

CVE-2024-6232 High

CVE-2024-6232 affects Python 3.10.10 (64-bit)

There is a MEDIUM severity vulnerability affecting CPython. Regular expressions that allowed excessive backtracking during tarfile. TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives.

CVSS v3 Score

7.500000

Availability: HIGH Confidentiality Impact: NONE Integrity Impact: NONE Privileges Required: NONE

Scope: UNCHANGED User Interaction: NONE

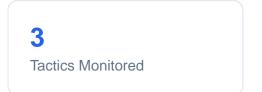
Affected Package

Python 3.10.10 (64-bit) (3.10.10150.0)

Architecture:

Published: September 3, 2024 Updated: September 5, 2024

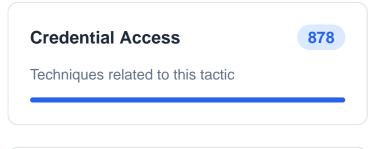
Security monitoring covers **3 MITRE ATT&CK tactics** and **2 unique techniques**, with a total of **879 technique detections**. This analysis provides insights into potential adversary behaviors and helps identify areas for security improvements.

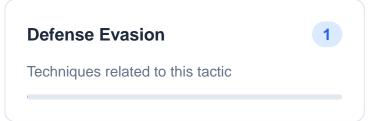


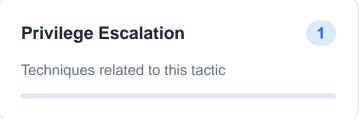
2 Unique Techniques



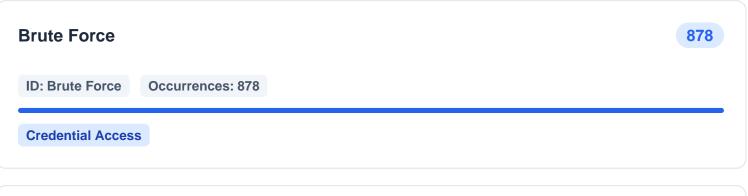
Tactics Coverage

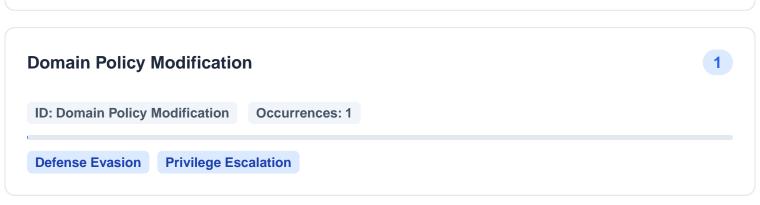






Top Techniques







Agent poc2_001 has reported 19 security events, including 0 high-severity alerts. The agent monitors 0 MITRE ATT&CK tactics and has detected 5 vulnerabilities.

Total Alerts
19

Security Events

High Severity

0

Critical Events

Compliance

3

Framework Controls

System Information

Agent ID

086

Agent Name

poc2_001

MITRE Coverage

0 Tactics

Vulnerabilities

5

Top Rules





Recent Alerts

2024/11/12 H11:10:15

2024/11/18 H10:55:04 Level 10 Multiple Windows error application events. 2024/11/18 H10:54:42 Level 10 Multiple Windows error application events. 2024/11/17 H1:02:13 Level 10 Multiple Windows error application events. 2024/11/15 H10:04:06 Level 10 Multiple Windows error application events. 2024/11/12 H4:05:11 Level 10 Multiple Windows error application events. 2024/11/12 H11:16:00 Level 10 Multiple Windows error application events. 2024/11/12 H11:11:45 Level 10 Multiple Windows error application events. 2024/11/12 H11:10:56 Level 10 Multiple Windows error application events.

Level 10

Multiple Windows error application events.

2024/11/12 H11:05:14

Level 10

Multiple Windows error application events.

Agent poc2_004 has reported 5 security events, including 0 high-severity alerts. The agent monitors 0 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

5

Security Events

High Severity

Critical Events

Compliance

Framework Controls

System Information

Agent ID

168

Agent Name

poc2_004

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules

Rule 61061

Level 10

Multiple Windows error application events.

windows windows_application

Recent Alerts

2024/11/26 H8:30:32

Level 10

Multiple Windows error application events.

2024/11/26 H4:31:58 Level 10

Multiple Windows error application events.

2024/11/26 H4:27:07

Level 10

Multiple Windows error application events.

2024/11/26 H3:55:45

Level 10

Multiple Windows error application events.

2024/11/26 H2:40:25

Level 10

Multiple Windows error application events.

Agent poc2_010 has reported 84 security events, including 10 high-severity alerts. The agent monitors 1 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

84

Security Events

High Severity

10

Critical Events

Compliance

5

Framework Controls

System Information

Agent ID

173

Agent Name

poc2_010

MITRE Coverage

1 Tactics

Vulnerabilities

0

Top Rules



Recent Alerts

2024/11/27 H4:17:50

Multiple Windows Logon Failures

Credential Access

2024/11/27 H4:17:50 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H4:17:49 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H4:17:49 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H4:17:49 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H4:17:49 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H4:17:49 Level 12 Multiple Windows Logon Failures Credential Access 2024/11/27 H3:31:01 Level 12 Multiple Windows Logon Failures **Credential Access**

2024/11/27 H3:31:01 Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H3:31:01

Level 12

Multiple Windows Logon Failures

Credential Access

Agent poc2_012 has reported 285 security events, including 10 high-severity alerts. The agent monitors 1 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

285

Security Events

High Severity

10

Critical Events

Compliance

5

Framework Controls

System Information

Agent ID

175

Agent Name

poc2_012

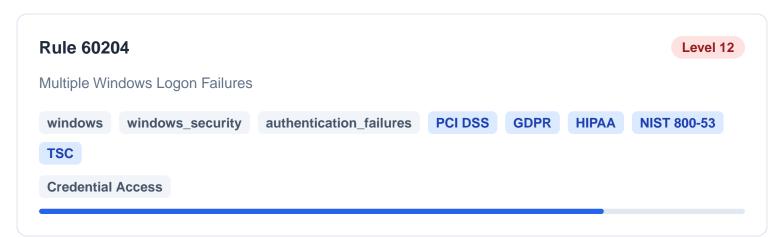
MITRE Coverage

1 Tactics

Vulnerabilities

0

Top Rules



Recent Alerts

2024/11/26 H4:29:57

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:29:37 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/26 H4:29:27 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/26 H4:29:07 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/26 H4:28:57 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/26 H4:28:37 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/26 H4:28:17 Level 12 Multiple Windows Logon Failures Credential Access 2024/11/26 H4:28:07 Level 12 Multiple Windows Logon Failures **Credential Access**

2024/11/26 H4:27:47 Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/26 H4:27:37

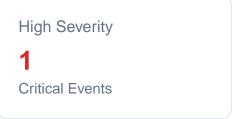
Level 12

Multiple Windows Logon Failures

Credential Access

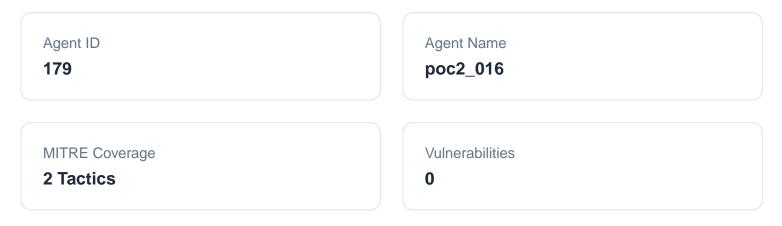
Agent poc2_016 has reported 1 security events, including 1 high-severity alerts. The agent monitors 2 MITRE ATT&CK tactics and has detected 0 vulnerabilities.







System Information



Top Rules



Recent Alerts



Agent poc2_017 has reported 2 security events, including 0 high-severity alerts. The agent monitors 0 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

Security Events

High Severity

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

180

Agent Name

poc2_017

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules



Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/26 H6:44:25

Level 10

Multiple System error events

2024/11/26 H6:41:18 Level 10

Multiple System error events

Agent poc2_029 has reported 514 security events, including 10 high-severity alerts. The agent monitors 1 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

514

Security Events

High Severity

10

Critical Events

Compliance

5

Framework Controls

System Information

Agent ID

192

Agent Name

poc2_029

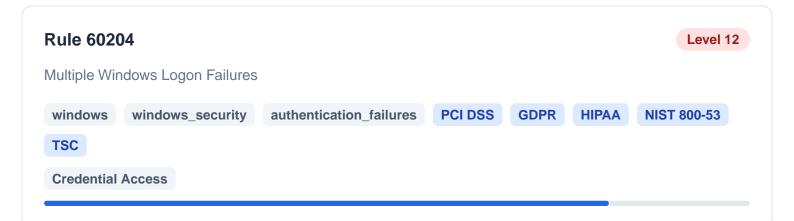
MITRE Coverage

1 Tactics

Vulnerabilities

0

Top Rules





Recent Alerts

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:49:33 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H1:44:33 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H1:39:33 Level 12 Multiple Windows Logon Failures Credential Access 2024/11/27 H1:34:32 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H1:34:32 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H1:34:32 Level 12 Multiple Windows Logon Failures **Credential Access** 2024/11/27 H1:34:26 Level 12 2024/11/27 H1:31:52 Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:31:13

Level 12

Multiple Windows Logon Failures

Credential Access

2024/11/27 H1:31:13

Level 12

Multiple Windows Logon Failures

Credential Access

Agent poc2_030 has reported 5 security events, including 0 high-severity alerts. The agent monitors 0 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

5

Security Events

High Severity

Critical Events

Compliance

0

Framework Controls

System Information

Agent ID

193

Agent Name

poc2_030

MITRE Coverage

0 Tactics

Vulnerabilities

0

Top Rules



Multiple System error events

windows windows_system

Recent Alerts

2024/11/27 H8:02:32

Level 10

Level 10

Multiple System error events

2024/11/27 H7:50:07

Multiple System error events

2024/11/27 H7:50:06

Multiple System error events

2024/11/27 H7:49:30

Multiple System error events

2024/11/27 H7:49:18

Multiple System error events

Agent poc2_031 has reported 6 security events, including 0 high-severity alerts. The agent monitors 0 MITRE ATT&CK tactics and has detected 0 vulnerabilities.

Total Alerts

6
Security Events

High Severity

O

Critical Events

Compliance

O

Framework Controls

System Information

Agent ID
194

MITRE Coverage
0 Tactics

Agent Name
poc2_031

Vulnerabilities
0

Top Rules



Recent Alerts

2024/11/27 H8:03:55

Multiple System error events

2024/11/27 H8:03:09 Level 10 Multiple System error events 2024/11/27 H8:02:23 Level 10 Multiple System error events 2024/11/26 H7:19:34 Level 10 Multiple System error events 2024/11/26 H5:37:50 Level 10 Multiple System error events 2024/11/26 H5:37:50 Level 10 Multiple System error events