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

Generated on
November 28, 2024

Powered by
SenseL Copilot Analytics

CONTENTS

OVERVIEW

AGENT ANALYSIS

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**.

Security Score	Active Agents	Total Alerts
0	9	921
Critical	of 41 Total	Security Events

Security Events Distribution

Critical Vulnerabilities	0
High Severity Alerts	879
Medium Severity Alerts	42

Security Coverage

MITRE Tactics Covered	3
Active Monitoring	9 Agents
Total Vulnerabilities	5

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	5	0
Critical Vulnerabilities	High Severity	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.

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: 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.

3	2	879
Tactics Monitored	Unique Techniques	Total Detections

Tactics Coverage

Credential Access 878

Techniques related to this tactic

Defense Evasion 1

Techniques related to this tactic

Privilege Escalation 1

Techniques related to this tactic

Top Techniques

Brute Force 878

ID: Brute Force | Occurrences: 878

Credential Access

Domain Policy Modification 1

ID: Domain Policy Modification | Occurrences: 1

Defense Evasion | Privilege Escalation

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	High Severity	Compliance
19	**0**	**3**
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
086	**poc2_001**

MITRE Coverage	Vulnerabilities
0 Tactics	**5**

Top Rules

Rule 61061

Level 10

Multiple Windows error application events.

windows windows_application

Rule 23505

Level 10

CVE-2024-6345 affects setuptools

vulnerability-detector PCI DSS GDPR TSC

Recent Alerts

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.

2024/11/12 H11:10:15 — 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	High Severity	Compliance
5	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
168	poc2_004

MITRE Coverage	Vulnerabilities
0 Tactics	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	High Severity	Compliance
84	**10**	**5**
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
173	**poc2_010**

MITRE Coverage	Vulnerabilities
1 Tactics	**0**

Top Rules

Rule 60204

Level 12

Multiple Windows Logon Failures

windows | windows_security | authentication_failures | PCI DSS | GDPR | HIPAA | NIST 800-53 | TSC

Credential Access

Recent Alerts

2024/11/27 H4:17:50

Level 12

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	High Severity	Compliance
285	**10**	**5**
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
175	**poc2_012**

MITRE Coverage	Vulnerabilities
1 Tactics	**0**

Top Rules

Rule 60204

Level 12

Multiple Windows Logon Failures

windows | windows_security | authentication_failures | PCI DSS | GDPR | HIPAA | NIST 800-53 | TSC

Credential Access

Recent Alerts

2024/11/26 H4:29:57

Level 12

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**.

Total Alerts	High Severity	Compliance
1	1	5
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
179	poc2_016

MITRE Coverage	Vulnerabilities
2 Tactics	0

Top Rules

Rule 60154

Level 12

Administrators Group Changed

windows windows_security group_changed win_group_changed PCI DSS GDPR HIPAA NIST 800-53 TSC

Defense Evasion Privilege Escalation

Recent Alerts

2024/11/27 H5:56:32

Level 12

Administrators Group Changed

Defense Evasion Privilege Escalation

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	High Severity	Compliance
2	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
180	poc2_017

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61110

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	High Severity	Compliance
514	**10**	**5**
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
192	**poc2_029**

MITRE Coverage	Vulnerabilities
1 Tactics	**0**

Top Rules

Rule 60204

Level 12

Multiple Windows Logon Failures

windows · windows_security · authentication_failures · PCI DSS · GDPR · HIPAA · NIST 800-53 · TSC

Credential Access

Rule 61110

Level 10

Multiple System error events

windows · windows_system

Recent Alerts

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**

Multiple Windows Logon Failures

Credential Access

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	High Severity	Compliance
5	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
193	poc2_030

MITRE Coverage	Vulnerabilities
0 Tactics	0

Top Rules

Rule 61110

Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/27 H8:02:32

Level 10

Multiple System error events

2024/11/27 H7:50:07

Level 10

Multiple System error events

2024/11/27 H7:50:06

Level 10

Multiple System error events

2024/11/27 H7:49:30

Level 10

Multiple System error events

2024/11/27 H7:49:18

Level 10

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	High Severity	Compliance
6	0	0
Security Events	Critical Events	Framework Controls

System Information

Agent ID	Agent Name
194	**poc2_031**

MITRE Coverage	Vulnerabilities
0 Tactics	**0**

Top Rules

Rule 61110

Level 10

Multiple System error events

windows windows_system

Recent Alerts

2024/11/27 H8:03:55

Level 10

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