# Standard Operating Procedure (SOP) Status for Threat Intelligence

## SOP Status of Operational Intelligence in December 2024

|  |  |  |  |
| --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Responsible Person |
| Cyber Threat Operations (CTO) | 3rd Modification of Latest Endorsement (Released on 16 Jan 2025)  Add  •Dark Web Monitoring Alerts Handling  - On working days at 10:00 AM and 4:00 PM, the TI on-site analyst will monitor alerts from Dark Web Monitoring (DWM) in the PwC JIRA Platform  - Created dark web monitoring alert ticket in JIRA ticket with title, component,  Modified  •High / Critical Case Follow Up  - Requested by AD(IT)(ITS)3, set the component of JIRA sub-ticket to “TI alert escalation” instead of “TI follow up” to track progress of system owner for further follow up | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |
| Security Operations Centre (SOC) | Last Modification of Latest Version (in 05 Nov 2024) | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |
| Threat Hunting | Last Modification of Latest Version (in 20 Dec 2024) | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |
| Incident Response (IR) | Last Modification of Latest Version (in 31 Jul 2024) | Latest endorsement on 05 Nov 2024, made by AD(IT)(ITS)3 on 13 Nov 2024 | PwC, HKMA |

# Cyber Threat Operations (CTO)

## 12.1 Monthly CVEs Summary

In December 2024, there were **1** high-security-level Common Vulnerabilities and Exposures (CVE), **8** medium-security-level CVE, **no** low-security-level CVE.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE number | Product | Summary | User Confirm Affected |
| High | PwC, GovCERT, CISA | 31/12/2024 | ITSSOC-8646 | CVE-2024-3393 | PAN-OS Firewall | Actively Exploited PAN-OS Firewall Denial of Service (DoS) Vulnerability | User confirmed not affected |
| Medium | PwC | 02/12/2024 | ITSSOC-8290 | CVE-2024-8929 | PHP | PoC Released for PHP Fake MySQL Server Connection or Network Tampering Leading to Arbitrary Code Execution | N/A |
| Medium | PwC | 02/12/2024 | ITSSOC-8291 | CVE-2024-11477 | 7-Zip | 7-Zip Zstandard Decompression Integer Underflow Remote Code Execution Vulnerability | N/A |
| Medium | PwC | 10/12/2024 | ITSSOC-8383 | CVE-2024-40717 | Veeam | Veeam Backup & Replication Script Execution Vulnerability | N/A |
| Medium | PwC, GovCERT | 11/12/2024 | ITSSOC-8395 | CVE-2024-53247 | Microsoft Products | Multiple Vulnerabilities in Microsoft Products (December 2024) for subscribers | N/A |
| Medium | PwC, GovCERT | 13/12/2024 | ITSSOC-8439 | CVE-2024-53247 | Splunk Secure Gateway App | Splunk Secure Gateway App Remote Code Execution Vulnerability | N/A |
| Medium | PwC | 13/12/2024 | ITSSOC-8444 | CVE-2024-11274 | GitLab | GitLab CE/EE Session Data Exfiltration Vulnerability | N/A |
| Medium | PwC | 18/12/2024 | ITSSOC-8516 | CVE-2024-55949 | MinIO | MinIO IAM import API Uncovers Privilege Escalation Vulnerability | N/A |
| Medium | PwC | 23/12/2024 | ITSSOC-8579 | CVE-2024-12727 | Sophos Firewall | Multiple Vulnerabilities in Sophos Firewall | N/A |

## 

## 12.2 Monthly High Severity Level CVEs Tracking

In December 2024, there were **no** High Severity Level CVEs affecting HKMA. The affected systems/servers and their scheduled patch dates were tracked by the respective system owners.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CVE number | Product | Response from System Owner | | | | Recommendations by PwC |
| Internet Facing | Affected System/ Server IP | Solution | Target Solution Apply Date |
| N/A | N/A | N/A | N/A | N/A | N/A | N/A |

## Remark: Only the product running the affected version are shown.

## 12.3 Ongoing CVEs Remediation (Until 17 Jan 2025)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Jira Ticket Number | CVE Number | Product Impacted | Severity | System Owner Name(s) | Date Raised by SOC | SOC Follow-up Attempts (1,2,3) | Date of Acknowledgement | Date of Last Follow-up | CVE Relevant to HKMA | Affected System/ Server IP | Target Remediation Completion Date | Actual Remediation Date | Time from Date Raised to Date Acknowledged (days) | Time from Date Acknowledged to Date Remediated (days) | Aging of Actual Remediation Date to Target Remediation Completion Date (days) | Source of Alert |
| ITSSOC-7772 | CVE-2024-23113 | FortiOS  FortiPAM  FortiProxy  FortiWeb | High | A(SYS)(IT)(IS)10 | 15 Oct 2024 | 1 | 17 Oct 2024 | 1st Follow-up: 29 Nov 20241 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | N/A | 3 | 933 | N/A | PwC, GovCERT |
| ITSSOC-7888 | CVE-2024-47575 | FortiManager | High | A(SYS)(IT)(IS)10 | 1st Attempt: 24 Oct 2024  2nd Attempt: 15 Nov 2024 | 2 | 15 Nov 2024 | 1st Follow-up: 29 Nov 20241  2nd Follow-up: 3 Jan 20252 | Yes | 172.20.22.23  172.20.141.23 | Dec 2024 | 12 Dec 2024 | 23 | 50 | 0 | PwC, GovCERT |
| ITSSOC-8114 | CVE-2024-0012 & CVE-2024-9474 | PAN-OS | High | Sr D(IT)(IS) | 15 Nov 2024 | 1 | 15 Nov 2024 | 1st Follow-up: 05 Dec 20241 | Yes | 172.22.48.101  172.22.48.102  172.22.48.105  172.22.48.111  172.22.48.112  172.22.49.101  172.22.49.102  172.22.49.105  172.22.49.111  172.22.49.112 | Q1 2025 | N/A | 1 | 643 | N/A | PwC, GovCERT, CISA |

As of December 2024, there were **3** ongoing CVEs remediation efforts.

Remarks:

1 First Follow-Up: SOC requested information from the system owner regarding the CVE.

2 Second Follow-Up: SOC inquired about the system owner's patch status.

3 The timeframe is calculated up to 17 Jan 2025; additional days will continue to be added until the patch is completed.

## 12.4 Major Threat Intelligence Report Highlight

This section shared major threat intelligence highlights for the past month.

1. Japan Airlines Under Cyberattack on 26 December, Flights Delayed
2. Actively Exploited Unauthenticated Denial of Service (DoS) Vulnerability in DNS Security Feature of Palo Alto Networks Firewall (CVE-2024-3393)

12.5 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | SOC Recommendation/Actionable Item |
| 1. Japan Airlines Under Cyberattack on 26 December, Flights Delayed | * Monitor and gain insights from the news related to the Japan Airlines cyberattack, which may be relevant to HKMA. |
| 1. Actively Exploited Unauthenticated Denial of Service (DoS) Vulnerability in DNS Security Feature of Palo Alto Networks Firewall (CVE-2024-3393) | * Send an email to the network team to confirm if their current version of the PA Firewall is impacted. |

1. Japan Airlines Under Cyberattack on 26 December, Flights Delayed

On 26 December 2024, Japan Airlines was impacted by a cyberattack resulting in operational disruptions. According to public reporting, the attack was suspected to have been a Distributed Denial of Service (DDoS) attack. This is based on Japan Airline's tweet indicating the "issue was due to a large data attack and did not result in any customer data leaks or virus infections".

**Impact and Analysis**

The attack caused delays and cancellations of flights, but did not result in malware deployment or data theft, confirmed by Japan Airlines at this time. In response to the attack, Japan Airlines temporarily disabled the impacted router and suspended ticket sales for flights departing on 26 December.

As of 17 January 2025, PwC has not observed any data breach or sales listed on the dark web for Japan Airlines.

This is not the first instance of an airline being impacted by a DDoS attack. In January 2024, AerCap suffered a ransomware attack resulting in data theft, and in March, Air Europa experienced a similar attack, indicating a trend of increasing cyber threats in the aviation sector.

At this time of writing, there is no Indicators of Compromise (IoCs) have been published. PwC will continue ongoing monitoring for any potential data breaches or updates, including any new information about the threat actors involved.

Source: [MingPao News](https://news.mingpao.com/ins/%e5%9c%8b%e9%9a%9b/article/20241226/s00005/1735178623878/%e6%97%a5%e8%88%aa%e7%b3%bb%e7%b5%b1%e4%b8%80%e5%ba%a6%e9%81%ad%e7%b6%b2%e7%b5%a1%e6%94%bb%e6%93%8a)

1. Actively Exploited Unauthenticated Denial of Service (DoS) Vulnerability in DNS Security Feature of Palo Alto Networks Firewall (CVE-2024-3393)

On 27 December 2024, Palo Alto Networks released a Security Advisory disclosing a new vulnerability impacting PAN-OS (CVE-2024-3393). The vulnerability enables an unauthenticated, remote attacker to achieve a Denial of Service (DoS) by sending a specially crafted packet through the firewall's data plane, disrupting firewall operations and forcing them into maintenance mode. Palo Alto Networks has confirmed active exploitation of this vulnerability in production environments.

**Impact and Analysis**

Palo Alto Networks is aware of customers experiencing this denial of service (DoS) when their firewall blocks malicious DNS packets that trigger this issue. However, it has not disclosed specific technical details regarding the mechanics of the vulnerability or the precise conditions under which it can be exploited.

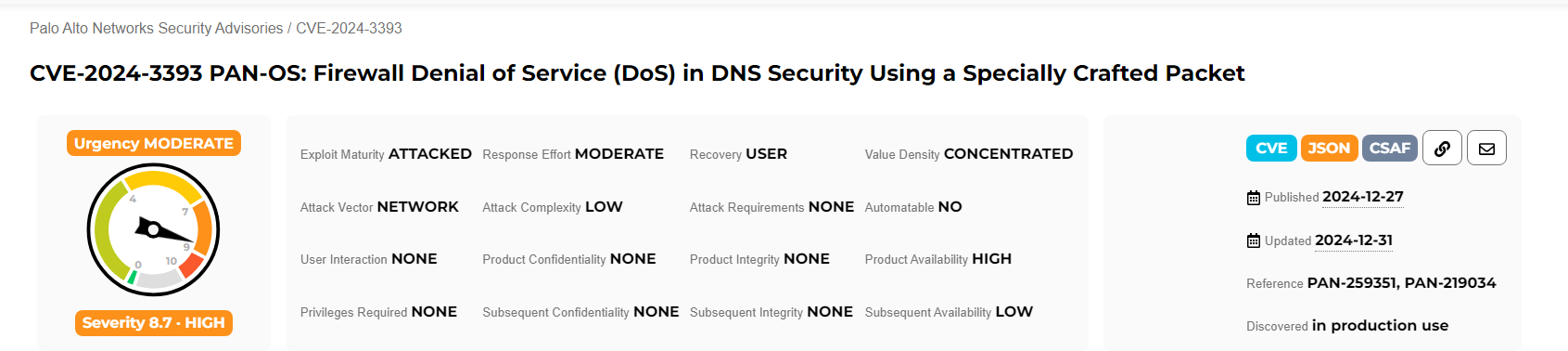
As of the time of writing, there are no indicators of compromise (IOCs) related to the CVE-2024-3393 vulnerability.

Affected Products:

* PAN-OS 11.2: Affected versions < 11.2.3
* PAN-OS 11.1: Affected versions < 11.1.5
* PAN-OS 10.2: Affected versions >= 10.2.8, < 10.2.10-h12, < 10.2.13-h2
* PAN-OS 10.1: Affected versions >= 10.1.14, < 10.1.14-h8
* Prisma Access: Affected versions >= 10.2.8 on PAN-OS< 11.2.3 on PAN-OS

\*Note: PAN-OS 11.0 reached the end of life (EOL), PA did not provide a fix for this release.

Source: [Palo Alto Network Security Advisory](https://security.paloaltonetworks.com/CVE-2024-3393)



# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In December 2024, a total of **14** threat hunting cases were handled. These included **5** government-targeted cases, **9** APAC-targeted cases, and **5** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
| 02/12/2024 | ITSSOC-8284 | New CleverSoar Installer Targets Chinese Users |  | ✓ |  |
| 03/12/2024 | ITSSOC-8301 | SmokeLoader's Advanced Tactics Targeted IT Industry in APAC Campaign |  | ✓ | ✓ |
| 04/12/2024 | ITSSOC-8305 | New Detection of Melofee Variant by Chinese APT Group | ✓ | ✓ | ✓ |
| 04/12/2024 | ITSSOC-8306 | Threat Actors Targeting Misconfigured Docker Remote API Servers With The Gafgyt Malware |  |  | ✓ |
| 05/12/2024 | ITSSOC-8323 | New C2 Cluster Targets APAC Industries |  | ✓ |  |
| 09/12/2024 | ITSSOC-8360 | Secret Blizzard Hijack C2 Infrastructure Target Against Governmental Organizations | ✓ |  |  |
| 12/12/2024 | ITSSOC-8428 | Zloader Trojan DNS Tunneling Protocol for Enhanced Evasion |  | ✓ |  |
| 17/12/2024 | ITSSOC-8511 | Ransomware LockBit 3.0 and Other Open-Source Tooling Observed in Asia Pacific | ✓ | ✓ |  |
| 24/12/2024 | ITSSOC-8606 | APT Group Parasite (APT-C-68) Targets Government Organizations | ✓ |  |  |
| 27/12/2024 | ITSSOC-8617 | LITTLELAMB.WOOLTEA Backdoor Discovered in Palo Alto Devices |  |  | ✓ |
| 31/12/2024 | ITSSOC-8647 | Malicious Package "Zebo-0.1.0" Found on Python Package Index (PyPI) |  | ✓ | ✓ |
| 31/12/2024 | ITSSOC-8648 | Emerging Ransomware Family NotLockBit Takes Inspiration from the Infamous LockBit |  |  |  |
| 31/12/2024 | ITSSOC-8650 | Lazarus Group's Latest Malware Campaign | ✓ | ✓ |  |
| 31/12/2024 | ITSSOC-8652 | The “You She” Group Distributes Malicious Installers against Chinese Users |  | ✓ |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

In December 2024, a total of **14** threat hunting cases were handled.

In addition, this effort resulted in the blocking of **84** hashes, **22** domains or URLs, and **49** IP addresses. All Indicators of Compromise (IoCs) were blocked, with **no** left unblocked.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Hits | Hash Blocked Count | Domain/URL Blocked Count | IP Blocked Count |
| 02/12/2024 | ITSSOC-8284 | New CleverSoar Installer Targets Chinese Users | N/A | 1 | 1 | 1 |
| 03/12/2024 | ITSSOC-8301 | SmokeLoader's Advanced Tactics Targeted IT Industry in APAC Campaign | N/A | 18 | 0 | 4 |
| 04/12/2024 | ITSSOC-8305 | New Detection of Melofee Variant by Chinese APT Group | N/A | 2 | 2 | 0 |
| 04/12/2024 | ITSSOC-8306 | Threat Actors Targeting Misconfigured Docker Remote API Servers With The Gafgyt Malware | N/A | 10 | 13 | 2 |
| 05/12/2024 | ITSSOC-8323 | New C2 Cluster Targets APAC Industries | N/A | 15 | 2 | 4 |
| 09/12/2024 | ITSSOC-8360 | Secret Blizzard Hijack C2 Infrastructure Target Against Governmental Organizations | N/A | 0 | 0 | 35 |
| 12/12/2024 | ITSSOC-8428 | Zloader Trojan DNS Tunneling Protocol for Enhanced Evasion | N/A | 13 | 3 | 1 |
| 17/12/2024 | ITSSOC-8511 | Ransomware LockBit 3.0 and Other Open-Source Tooling Observed in Asia Pacific | N/A | 8 | 0 | 1 |
| 24/12/2024 | ITSSOC-8606 | APT Group Parasite (APT-C-68) Targets Government Organizations | N/A | 2 | 1 | 1 |
| 27/12/2024 | ITSSOC-8617 | LITTLELAMB.WOOLTEA Backdoor Discovered in Palo Alto Devices | N/A | 1 | 0 | 0 |
| 31/12/2024 | ITSSOC-8647 | Malicious Package "Zebo-0.1.0" Found on Python Package Index (PyPI) | N/A | 1 | 0 | 0 |
| 31/12/2024 | ITSSOC-8648 | Emerging Ransomware Family NotLockBit Takes Inspiration from the Infamous LockBit | N/A | 5 | 0 | 0 |
| 31/12/2024 | ITSSOC-8650 | Lazarus Group's Latest Malware Campaign | N/A | 6 | 0 | 0 |
| 31/12/2024 | ITSSOC-8652 | The “You She” Group Distributes Malicious Installers against Chinese Users | N/A | 2 | 0 | 0 |
| Total | | | | 84 | 22 | 49 |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were 12 of reported emails from Communications Division in December, 2024.

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Category |
| 02/12/2024 | ITSPEIR-3567 | Clickbait | Spam |
| 03/12/2024 | ITSPEIR-3569 | Request for Reply | Spam |
| 04/12/2024 | ITSPEIR-3572 | Credential Harvesting | Phishing |
| 09/12/2024 | ITSPEIR-3578 | Request for Reply | Spam |
| 10/12/2024 | ITSPEIR-3580 | Credential Harvesting | Phishing |
| 12/12/2024 | ITSPEIR-3582 | Clickbait | Spam |
| 12/12/2024 | ITSPEIR-3584 | Financial Scam | Spam |
| 12/12/2024 | ITSPEIR-3586 | Financial Scam | Spam |
| 16/12/2024 | ITSPEIR-3594 | Request for Data | Spam |
| 19/12/2024 | ITSPEIR-3596 | Clickbait | Spam |
| 23/12/2024 | ITSPEIR-3606 | Financial Scam | Spam |
| 23/12/2024 | ITSPEIR-3608 | Request for Data | Spam |
| 27/12/2024 | ITSPEIR-3613 | Impersonation Scam | Spam |
| 27/12/2024 | ITSPEIR-3614 | Impersonation Scam | Spam |
| 27/12/2024 | ITSPEIR-3615 | Impersonation Scam | Spam |
| 27/12/2024 | ITSPEIR-3617 | Financial Scam | Spam |

## 14.2 Settlement Division

There were 8 of reported emails from Settlement Division in December, 2024.

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Category |
| 13/12/2024 | ITSPEIR-3588 | Clickbait | Spam |
| 16/12/2024 | ITSPEIR-3590 | Financial Scam | Spam |
| 16/12/2024 | ITSPEIR-3592 | Clickbait | Spam |
| 23/12/2024 | ITSPEIR-3598 | Credential Harvesting | Phishing |
| 23/12/2024 | ITSPEIR-3599 | Credential Harvesting | Phishing |
| 23/12/2024 | ITSPEIR-3600 | Credential Harvesting | Phishing |
| 23/12/2024 | ITSPEIR-3604 | Clickbait | Spam |
| 27/12/2024 | ITSPEIR-3611 | Clickbait | Spam |

## 14.3 Overview

In December 2024, TI has acknowledged **20** suspicious email reports by users, confirming that there are **0** unwanted emails, **15** spam emails, and **5** phishing emails. TI has sent out emails to the users who reported these emails, advising them to delete these emails and avoid clicking on any links or attachments within them. Additionally, instructions were provided on how to block future emails from the same sender to prevent further phishing attempts.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unwanted | Spam | Phishing |
| Communications Division | 0 | 10 | 2 |
| Settlements Division | 0 | 5 | 3 |
| Total | 0 | 15 | 5 |