# Standard Operating Procedure (SOP) Status for Threat Intelligence

## SOP Status of Operational Intelligence in October 2025

|  |  |  |  |
| --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Responsible Person |
| Cyber Threat Operations (CTO) | Last Modification of Latest Version (On 28 Jul 2025) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Security Operations Centre (SOC) | Last Modification of Latest Version (On 05 Nov 2024) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Threat Hunting | Last Modification of Latest Version (On 26 Mar 2025) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |
| Incident Response (IR) | Last Modification of Latest Version (On 31 Jul 2024) | Latest endorsement on 25 Feb 20251 | PwC, HKMA |

Remarks:

1 Since no further comment listed in SOC Monthly Meeting on 25 Feb 2025, the latest version of SOP for Threat Intelligence – “HKMA Threat Intelligence SOP – 20250224” is endorsed.

# Cyber Threat Operations (CTO)

## 12.1 Monthly CVEs Summary

In September 2025, there were **1** critical& **7** high-severity-level Common Vulnerabilities and Exposures (CVEs).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE number | Product | Summary | User Reply |
| High | PwC, | 19/09/2025 | ITSSOC-11490 | CVE-2025-6203 | HashiCorp Vault | HashiCorp Vault Denial of Service Through Complex JSON Payloads | N/A |
| High | PwC | 19/09/2025 | ITSSOC-11491 | CVE-2025-10491 | MongoDB | Improper Access Control in MongoDB Windows Installation | N/A |
| High | PwC, DPO | 19/09/2025 | ITSSOC-11492 | CVE-2025-10585 | Google Chrome | High Threat Security Alert (A25-09-14): Multiple Vulnerabilities in Google Chrome for subscribers | Affected |
| High | PwC, DPO | 19/09/2025 | ITSSOC-11493 | CVE-2025-43300 | iOS, macOS | High Threat Security Alert (A25-08-18): Vulnerability in Apple Products for subscribers | N/A |
| High | PwC | 19/09/2025 | ITSSOC-11499 | CVE-2025-5115 | Jenkins | Jenkins MadeYouReset HTTP/2 Denial of Service (DoS) Vulnerability | N/A |
| High | PwC | 25/09/2025 | ITSSOC-11525 | CVE-2025-20352 | Cisco IOS and IOS XE Software | Actively Exploited Cisco IOS and IOS XE Software Denial of Service and Remote Code Execution Vulnerability | N/A |
| Critical | PwC | 26/09/2025 | ITSSOC-11538 | CVE-2025-20333, CVE-2025-20362 | Cisco ASA Software | Zero-Day Cisco ASA and FTD Remote Code Execution via Chain Exploit | N/A |
| High | PwC | 29/09/2025 | ITSSOC-11546 | CVE-2025-54831 | Cisco Firepower Threat Defense | Apache Airflow Vulnerability Exposes Sensitive Details to Read-Only Users | N/A |

## 12.2 Monthly High Severity Level CVEs Tracking

In September 2025, there were **1** 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 |
| CVE-2025-10585 | Google Chrome | N/A | HKFMI-WPS-PD1  HKFMI-CMS-UA1  RTGS-DATA-UAT  RTGS-MIS-UAT  SHCHGW-WS-PD  SFTPGW-WS-DR  HKFMI-RPA-BR1  HKFMI-RPA-BR2 | Upgraded to version 140.0.7339.186 | 04 Oct 2025 | Install a patch to fully remediate the sandbox security feature bypass vulnerability. No workaround is available.  Update to 140.0.7339.185/.186 for Windows/Mac, and 140.0.7339.185 for Linux. |

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

## 12.3 Ongoing CVEs Remediation (Until 27 Oct 2025) 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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-9623 | CVE-2025-2783 | Google Chrome | Critical3 | AD(IT)(PSM)1 | 1st Attempt: 26 Mar 2025  2nd Attempt: 16 September 2025 | 2 | 16 September 2025 | N/A | Yes | N/A | Within 6 weeks | Pending | 0 | 71**1** | N/A | PwC, DPO |

As of September 2025, there were **1** ongoing CVEs remediation efforts.

Remarks:

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

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

**1** The timeframe is calculated up to 27 Oct 2025; additional days will continue to be added until the patch is completed.

**2**Team is currently in the development and testing phase of the system. The user has agreed to provide an update once the impact analysis is complete.

## 12.4 Completed CVEs Remediation (Until 27 Oct 2025)

As of September 2025, there were **10** completed CVEs remediation efforts.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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-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 2024  2nd Follow-up: 3 Jan 2025 | Yes | 172.20.22.23  172.20.141.23 | Dec 2024 | 12 Dec 2024 | 23 | 50 | 0 | PwC, GovCERT |
| ITSSOC-8780 | CVE-2024-55591, CVE-2025-24472 | FortiOS  FortiProxy | High | A(SYS)(IT)(IS)10 | 15 Jan 2025 | 1 | 15 Jan 2025 | 1st Follow-up: 16 Jan 2025; 20 Jan 2025  2nd Follow-up: 14 Feb 2025 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | KCC: 8 Feb 2025  IFC: 15 Feb 2025 | 1 | 31 | 0 | PwC, GovCERT, CISA |
| 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 2024 | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | Feb 2025 | 17 Feb 2025 | 3 | 125 | 0 | PwC, GovCERT |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(AS2)2 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025  4th Attempt: 03 Mar 2025 | >3 | 05 Mar 2025 | 1st Follow-up: 6 Mar 2025; 7 Mar 2025 | Yes | 172.31.234.105 | Before 12 Mar 2025 | 10 Mar 2025 | 15 | 5 | 0 | PwC |
| 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 2024 | 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 | 31 Mar 2025 | 1 | 136 | 0 | PwC, GovCERT, CISA |
| ITSSOC-9180 | CVE-2025-1094 | PostgreSQL | High | AD(IT)(PSM)1 | 1st Attempt: 19 Feb 2025  2nd Attempt: 21 Feb 2025  3rd Attempt: 25 Feb 2025  4th Attempt: 03 Mar 2025 | >3 | 04 Mar 2025 | 1st Follow-up: 5 Mar 2025; 11 Mar 2025 | Yes | 172.31.110.180  172.31.91.87  172.31.151.51  172.31.110.253  172.31.161.62 | Within 180 days | 03 September 2025 | 14 | 61 | 0 | PwC |
| ITSSOC-10536 | CVE-2025-5419 | Google Chrome | High | D(IT)(ITS)2 | 1st Attempt: 05 Jun 2025 | 1 | 11 Jun 2025 | N/A | Yes | PAM-CPM-PD1  PAM-CPM-PD2  PAM-PSM-PD1  PAM-PSM-PD2  PAM-CPM-DR  PAM-PSM-DR1  PAM-PSM-DR2  spamprdcm101  spamprdcm102  spamprdpm101  spamprdpm102  spamprdcm201  spamprdcm202  spamprdpm201  spamprdpm202 | 2 Jul 2025 | 2 Jul 2025 | 6 | 21 | 0 | PwC, DPO |
| ITSSOC-10975 | CVE-2025-41236  CVE-2025-41237  CVE-2025-41238 | ESXi  VMware Tools(Windows) | High | D(IT)(ITS)2 | 1st Attempt: 16 Jul 2025 | 1 | 23 Jul 2025 | N/A | Yes | PAM-CPM-PD1  PAM-PSM-PD1  PAM-CPM-PD2  PAM-PSM-PD2  PAM-CPM-DR  PAM-PSM-DR1  PAM-PSM-DR2  PAM-VAULT-TEST  PAM-CPM-TEST  PAM-PSM-TEST | 14 Aug 2025 | 14 Aug 2025 | 8 | 21 | 0 | PwC |
| ITSSOC-10975 | CVE-2025-41236  CVE-2025-41237  CVE-2025-41238 | VMware Tools(Windows) | High | D(IT)(ITS)2 | 1st Attempt: 16 Jul 2025 | 1 | 23 Jul 2025 | N/A | Yes | PAM-CPM-PD1  PAM-PSM-PD1  PAM-CPM-PD2  PAM-PSM-PD2  PAM-CPM-DR  PAM-PSM-DR1  PAM-PSM-DR2  PAM-VAULT-TEST  PAM-CPM-TEST  PAM-PSM-TEST | 28 Jul 2025 | 28 Aug 2025 | 8 | 35 | 0 | PwC |
| ITSSOC-10884 | CVE-2025-5419 | Palo Alto Firewall | High | A(SYS)(IT)(IS)10 | 1st Attempt: 11 Jul 2025  2nd Attempt: 14 Jul 2025 | 2 | 14 Jul 2025 | N/A | Yes | IFC OA  172.22.48.101  172.22.48.102  172.22.48.105  172.22.48.111  172.22.48.112  IFC SWT  172.22.148.51  172.22.148.52  172.22.148.55  KCC OA  172.22.49.101  172.22.49.102  172.22.49.105  172.22.49.111  172.22.49.112  KCC SWT  172.22.149.51  172.22.149.52  172.22.149.55 | 26/07 (KCC)  09/08 (IFC) | Before 09 September 2025 | 4 | 12**1** | 0 | PwC, DPO |
| ITSSOC-11492 | CVE-2025-10585 | Google Chrome | High | AD(FMIS)(IT)2 | 1st Attempt: 18 Sep 2025 | 1 | 24 Sep 2025 | N/A | Yes | HKFMI-WPS-PD1  HKFMI-CMS-UA1  RTGS-DATA-UAT  RTGS-MIS-UAT  SHCHGW-WS-PD  SFTPGW-WS-DR  HKFMI-RPA-BR1  HKFMI-RPA-BR2 | 04 Oct 2025 | 04 Oct 2025 | 7 | 10 | 0 | PwC, DPO |

Remarks:

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

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

## 12.5 Major Threat Intelligence Report Highlight

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

1. NPM Packages Supply‑Chain Compromise Affecting Chalk, Debug and Related Packages in a Supply Chain Attack
2. UTG-Q-010 Group's Supply Chain Attack Strike Directly at the Heart of Hong Kong's Financial Market

12.6 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | SOC Recommendation/Actionable Item |
| 1. Fortinet NPM Packages Supply‑Chain Compromise Affecting Chalk, Debug and Related Packages in a Supply Chain Attack | 1\ Confirm whether any CI/CD or local builds ran npm install/update for projects with these dependencies between 21:00–23:30 HKT on Sep 8, and review package-lock.json or pnpm-lock.yaml changes during that window.  2\ If your projects are being affected, please rollback to the last known safe versions of the affected packages (versions prior to those listed above).  3\ Report any findings of compromised packages or suspicious activity to ITS immediately, by replying this email. |
| 1. UTG-Q-010 Group's Supply Chain Attack Strike Directly at the Heart of Hong Kong's Financial Market | 1\ TI on-site analyst threat hunt campaign targeting malicious IP Addresses and Domains. Found no compromise within HKMA security solutions, and all known IoCs have been blocked. |

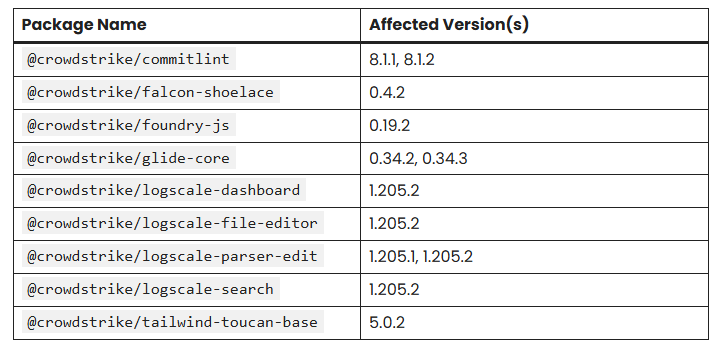
1. NPM Packages Supply‑Chain Compromise Affecting Chalk, Debug and Related Packages in a Supply Chain Attack

On September 15, the Node Package Manager (NPM) repository experienced an ongoing supply chain attack, in which the attackers executed a highly targeted phishing campaign to compromise the account of an NPM package maintainer. With privileged access, the attackers injected malicious code into widely used JavaScript packages, threatening the entire software ecosystem. Notably, the attack has disrupted several key NPM packages, including those integral to application development and cryptography.

**Impact and Analysis**

The incident, which involves the same malware previously used to target the popular tinycolor package, highlights the persistent threat of supply chain vulnerabilities within the open-source ecosystem.

The npm registry acted swiftly to remove the affected packages, but developers and organizations are urged to take immediate action to mitigate potential damage.



**Recommendations**

1\ Confirm whether any CI/CD or local builds ran npm install/update for projects with these dependencies between 21:00–23:30 HKT on Sep 8, and review package-lock.json or pnpm-lock.yaml changes during that window.

2\ If your projects are being affected, please rollback to the last known safe versions of the affected packages (versions prior to those listed above).

3\ Report any findings of compromised packages or suspicious activity to ITS immediately, by replying this email.

Source: CISA Alert on Widespread Supply Chain Compromise Impacting npm Ecosystem (<https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem>)

1. **UTG-Q-010 Group's Supply Chain Attack Strike Directly at the Heart of Hong Kong's Financial Market**

The UTG-Q-010 threat group has targeted Hong Kong's financial sector with supply chain attacks by infiltrating two gold trading platforms, Jinrong China and Wanzhou Gold. The attacks exploit high-value investors in the gold market, aiming to steal large sums of money or manipulate financial markets for profit. This supply chain campaign has involved victims from key industries such as finance, manufacturing and culture.

**Impact and Analysis**

The UTG-Q-010 group compromised trusted Hong Kong gold trading platforms: the servers of jrjr.hk (Jinrong China) and wzg.com (Wanzhou Gold) to serve tampered installation packages containing malware, such as upway\_desktop.exe and wzgoldgroup5setup.exe. These packages appeared legitimate to users downloading financial software directly from the official sites, luring high-value investors and enterprises into installing them for normal trading purposes.

The group was extremely vindictive and went so far as to launch a low-level spear-email attack against public email addresses.



**Recommendations**

1\ TI on-site analyst threat hunt campaign targeting malicious IP Addresses and Domains. Found no compromise within HKMA security solutions, and all known IoCs have been blocked.

Source: UTG-Q-010 Group's Supply Chain Attack Strike Directly at the Heart of HongKong's Financial Market (<https://ti.qianxin.com/blog/articles/utg-q-010-supply-chain-attacks-strike-directly-at-the-heart-of-hongkongs-financial-market-en/>)

# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In September 2025, a total of **5** threat hunting cases were handled. These included **3** government / financial-targeted cases, **3** APAC-targeted cases, and **2** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government / Financial Targeted | APAC Targeted | Technology Related |
| 05/09/2025 | ITSSOC-11353 | Open-Source Infostealer "Stealerium" Leveraged in Phishing Campaigns | ✓ | ✓ |  |
| 05/09/2025 | ITSSOC-11354 | UTG-Q-010 Threat Group Targeted Hong Kong's Financial Sector with Supply Chain Attacks | ✓ | ✓ |  |
| 11/09/2025 | ITSSOC-11401 | APT28 Uses GONEPOSTAL Malware Provides Backdoor Access to Microsoft Outlook |  |  | ✓ |
| 15/09/2025 | ITSSOC-11423 | SEO Poisoning Attack Targets Chinese-Speaking Users with Fake Software Sites |  | ✓ |  |
| 22/09/2025 | ITSSOC-11510 | "GOLD SALEM" Ransomware Group Is Exploiting SharePoint Flaws | ✓ |  | ✓ |

## 13.2 Indicators of Compromise (IOCs) Blocked

In September 2025, a total of **5** threat hunting cases were handled.

In addition, this effort resulted in the blocking of **20** hashes, **10** domains or URLs, **4** 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 |
| 05/09/2025 | ITSSOC-11353 | Open-Source Infostealer "Stealerium" Leveraged in Phishing Campaigns | No | 5 | 0 | 0 |
| 05/09/2025 | ITSSOC-11354 | UTG-Q-010 Threat Group Targeted Hong Kong's Financial Sector with Supply Chain Attacks | No | 1 | 1 | 0 |
| 11/09/2025 | ITSSOC-11401 | APT28 Uses GONEPOSTAL Malware Provides Backdoor Access to Microsoft Outlook | No | 2 | 0 | 0 |
| 15/09/2025 | ITSSOC-11423 | SEO Poisoning Attack Targets Chinese-Speaking Users with Fake Software Sites | No | 10 | 9 | 4 |
| 22/09/2025 | ITSSOC-11510 | "GOLD SALEM" Ransomware Group Is Exploiting SharePoint Flaws | No | 2 | 0 | 0 |
| Total | | | | 20 | 10 | 4 |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were **13** of reported emails from Communications Division in September 2025.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 01/09/2025 | ITSPEIR-4282 | Phishing |
| 02/09/2025 | ITSPEIR-4284 | Phishing |
| 05/09/2025 | ITSPEIR-4288 | Phishing |
| 05/09/2025 | ITSPEIR-4289 | Phishing |
| 05/09/2025 | ITSPEIR-4290 | Phishing |
| 08/09/2025 | ITSPEIR-4294 | Phishing |
| 09/09/2025 | ITSPEIR-4296 | Phishing |
| 09/09/2025 | ITSPEIR-4297 | Phishing |
| 09/09/2025 | ITSPEIR-4299 | Spam |
| 17/09/2025 | ITSPEIR-4301 | Phishing |
| 25/09/2025 | ITSPEIR-4305 | Phishing |
| 25/09/2025 | ITSPEIR-4307 | Phishing |
| 25/09/2025 | ITSPEIR-4308 | Phishing |

## 14.2 Settlement Division

There were **2** of reported emails from Settlement Division in September 2025.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 22/09/2025 | ITSPEIR-4303 | Spam |
| 26/09/2025 | ITSPEIR-4310 | Spam |

## 14.3 Overview

In September 2025, TI has acknowledged **15** suspicious email reports by users, confirming that there are **3** spam emails, and **12** 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.

|  |  |  |
| --- | --- | --- |
|  | Spam | Phishing |
| Communications Division | 1 | 12 |
| Settlements Division | 2 | 0 |
| Total | 3 | 12 |