# TI SOP Status

## SOP Status of Operational Intelligence in November (Until 27th Nov 2024)

|  |  |  |  |
| --- | --- | --- | --- |
| Content of SOP | Detail | Status | Responsible Person |
| Cyber Threat Operations (CTO) | 1st Modification of Latest Endorsement (Released on 27 Nov 2024)  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 05 Nov 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 Common Vulnerabilities and Exposures (CVEs)

In October 2024, there were **2** high-security-level Common Vulnerabilities and Exposures (CVE) and **16** medium-security-level CVE.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE Identifier | Summary | User Confirm Affected |
| High | PwC | 15/10/2024 | ITSSOC-7772 | CVE-2024-23113 | Fortinet FortiOS Format String Vulnerability | Confirmed by Network Team |
| High | GovCERT.HK, PwC | 24/10/2024 | ITSSOC-7888 | CVE-2024-47575 | FortiManager Missing Authentication Vulnerability | Confirmed by Network Team |
| Medium | PwC | 02/10/2024 | ITSSOC-7631 | CVE-2024-26808 | PoC Exploit Shows Local Privilege Escalation Risk in Linux | N/A |
| Medium | PwC | 02/10/2024 | ITSSOC-7630 | CVE-2024-43917 | Unpatched SQLi Flaw in WordPress TI WooCommerce | N/A |
| Medium | PwC | 03/10/2024 | ITSSOC-7650 | CVE-2024-20432 | Cisco Nexus Dashboard Fabric Controller Web UI Command Injection Vulnerability | N/A |
| Medium | PwC | 04/10/2024 | ITSSOC-7664 | CVE-2024-5102 | Avast Antivirus Flaw Could Allow Hackers to Delete Files and Run Code as SYSTEM | N/A |
| Medium | PwC | 04/10/2024 | ITSSOC-7663 | CVE-2024-47806 & CVE-2024-47807 | Jenkins OpenId Connect Authentication Plugin potentially gaining administrator access | N/A |
| Medium | PwC | 04/10/2024 | ITSSOC-7662 | CVE-2024-47561 | Apache Avro Java SDK: Arbitrary Code Execution when reading Avro Data | N/A |
| Medium | PwC | 04/10/2024 | ITSSOC-7661 | CVE-2024-8885 | Resolved LPE vulnerability in Sophos Intercept X for Windows | N/A |
| Medium | GovCERT.HK, PwC | 09/10/2024 | ITSSOC-7714 | CVE-2024-3596 | Vulnerability in Juniper Networks Junos OS and Junos OS Evolved | N/A |
| Medium | GovCERT.HK, PwC | 09/10/2024 | ITSSOC-7715 | CVE-2024-43572 & CVE-2024-43573 | Multiple Vulnerabilities in Microsoft Products (October 2024) for subscribers | N/A |
| Medium | GovCERT.HK, PwC | 10/10/2024 | ITSSOC-7734 | CVE-2024-9680 | Vulnerability in Firefox | N/A |
| Medium | GovCERT.HK, PwC | 10/10/2024 | ITSSOC-7735 | CVE-2024-9464 & CVE-2024-9465 | Multiple Vulnerabilities in Palo Alto Networks Expedition for subscribers | N/A |
| Medium | GovCERT.HK, PwC | 14/10/2024 | ITSSOC-7764 | CVE-2024-9164 | Multiple Vulnerabilities in GitLab | N/A |
| Medium | PwC | 15/10/2024 | ITSSOC-7773 | CVE-2024-47806 & CVE-2024-47807 | Splunk Enterprise Remote Code Execution (RCE) Vulnerability | Confirmed by ITS Team |
| Medium | PwC | 16/10/2024 | ITSSOC-7785 | CVE-2024-9486 | Kubernetes Image Builder Default Credentials Vulnerability | N/A |
| Medium | PwC | 18/10/2024 | ITSSOC-7815 | CVE-2024-9264 | Grafana SQL Expressions allow for remote code execution | N/A |
| Medium | GovCERT.HK, PwC | 28/10/2024 | ITSSOC-7918 | CVE-2024-20432 | Multiple Vulnerabilities in Cisco Products | N/A |

## 12.2 Follow-up on High Severity Level CVEs

There were 2 High Severity Level CVEs Affected HKMA in October 2024. Below implies the patch/workaround follow-up. The TI on-site analyst will keep monitoring the progress of applying workaround/patching from user.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CVE number | Product | Response from System Owner | | | | Recommendations by PwC |
| Internet Facing | Affected System/ Server IP | Schedule patch/ workaround date | Target Patch Date |
| CVE-2024-23113 | FortiOS / FortiPAM / FortiProxy / FortiWeb Wifi Firewall | Yes | 172.20.22.21  172.20.22.22  172.20.141.21  172.20.141.22 | 1) User has followed the workaround by firewall policy to control access to fgfm port (TCP\_541) and turn off fgfm on the internet facing interface followed by patch  2) User has planned to follow annual patch schedule for patch | Feb 2025 | The user should apply the patch after the implementation of workaround.  Justification  Please note that a local-in policy that only allows FGFM connections from a specific IP will reduce the attack surface, but it won’t prevent the vulnerability from being exploited from this IP. Consequently, this is not a complete workaround. |
| CVE-2024-47575 | FortiManager Wifi Firewall | No | 172.20.22.23  172.20.141.23 | User replied the following:  1) Two of our fortimanager is running the affected version and we have followed the workaround to mitigate the issue.  One of our fortimanager is running the affected version on the management subnet only, which is controlled by firewall policy and require management subnet access to perform the exploit.  2) The manager that has not followed the workaround is in discussion with our maintenance vendor to carry out the patch | Dec 2024 | All the mentioned FortiManager instances by users should follow the patch.  Justification  Given the active exploitation by threat actor and the public release of Proof-of-Concept (PoC), we assess other threat actors may exploit CVE-2024-47575. |

## 12.3 Major Threat Intelligence Report Highlight

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

1. Actively Exploited Fortinet Multiple Products Format String Bug Allows Critical RCE Vulnerability (CVE-2024-23113)
2. Zero Day Actively Exploited Fortinet FortiManager Missing Authentication Vulnerability, PoC Released (CVE-2024-47575)

12.4 Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | TI Recommendation/Actionable Item |
| 1. Actively Exploited Fortinet Multiple Products Format String Bug Allows Critical RCE Vulnerability (CVE-2024-23113) | * Send an outlook email to confirm if the network team was impacted * Follow-up with the users’ workaround/patch |
| 1. Zero Day Actively Exploited Fortinet FortiManager Missing Authentication Vulnerability, PoC Released (CVE-2024-47575) | * Send an outlook email to confirm if the network team was impacted * Follow-up with the users’ workaround/patch |

1. Actively Exploited Fortinet Multiple Products Format String Bug Allows Critical RCE Vulnerability (CVE-2024-23113)

On 8 February 2024, Fortinet released a Security Advisory disclosing a new vulnerability impacting multiple products, including FortiOS, FortiProxy, FortiPAM, and FortiWeb (CVE-2024-23113). The vulnerability enables an unauthenticated attacker to execute unauthorized code or commands via specially crafted packets. The Proof-of-Concept (PoC) was released on March 2024, whilst it has been recently listed on CISA’s Known Exploited Vulnerabilities Catalog on 9 October 2024.

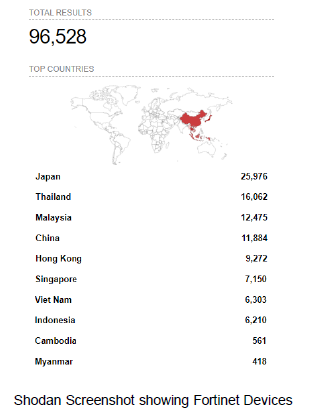
**Impact and Analysis**

CVE-2024-23113 is a pre-authentication Remote Code Execution (RCE) Vulnerability affecting the fgfmd daemon, was first disclosed and patched by Fortinet back in February 2024. This flaw allows remote, unauthenticated attackers to execute arbitrary code on vulnerable devices through simple attacks that require no user interaction, leading to the theft of sensitive data and the launch of further attacks from the compromised system.

As of 14 October 2024, we observe 96,528 exposed Fortinet across China mainland, Hong Kong, Macau, Malaysia, Japan, Indonesia, Singapore, Thailand, Vietnam, Cambodia and Myanmar.

Affected Products:

* FortiOS
* FortiPAM
* FortiProxy
* FortiWeb



2. Zero Day Actively Exploited Fortinet FortiManager Missing Authentication Vulnerability, PoC Released (CVE-2024-47575)

Fortinet issued a warning on 23 October 2024, regarding CVE-2024-47575, a severe zero-day flaw impacting their FortiManager network management system. This vulnerability enables remote unauthorized attackers to run malicious code or commands through carefully crafted requests. PwC’s Dark Lab urges impacted clients to apply the latest patch immediately, given active exploitation by threat actor “UNC5820”. (UPDATE) On 15 November 2024, Watchtowr released a Proof-of-Concept (PoC) named FortiJump for CVE-2024-47575. Given the release of a PoC and its unauthenticated nature, we assess other threat actors to exploit CVE-2024-47575.

**Impact and Analysis**

CVE-2024-47575 is a critical zero-day vulnerability affecting Fortinet’s FortiManager network management solution. This vulnerability arises from a missing authentication for a critical function [CWE-306] in the FortiManager fgfmd daemon, allowing remote unauthenticated attackers to execute arbitrary code or commands via specially crafted requests

Affected Products:

• FortiManager

# Threat Hunting

## 13.1 Threat Hunting Relevance and Overview

In October 2024, a total of **15** threat hunting cases were handled. These included **2** government-targeted cases, **3** APAC-targeted cases, and **9** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
| 09/10/2024 | ITSSOC-7716 | Fake Adobe Site in Phishing Emails Targets Enterprise Networks |  |  | ✓ |
| 10/10/2024 | ITSSOC-7724 | Contagious Interview Campaign Targeting Job-Seeking Individuals on LinkedIn |  |  | ✓ |
| 14/10/2024 | ITSSOC-7763 | DarkVision remote access trojan (RAT): A Rising Threat in Recent Cyber Campaigns |  |  |  |
| 15/10/2024 | ITSSOC-7774 | Red Team Tool EDRSilencer Disrupting Endpoint Security Solutions |  |  | ✓ |
| 17/10/2024 | ITSSOC-7802 | LockBit Ransomware Abuses AWS for Attack |  |  | ✓ |
| 18/10/2024 | ITSSOC-7806 | Horus FUD (Fully Un-Detectable) Crypter Malware Distributor for Various Threats |  |  |  |
| 21/10/2024 | ITSSOC-7819 | Social Engineering via CAPTCHA Validations: Exploiting Windows Keyboard Shortcuts Could Lead User to Trigger Malicious Commands |  | ✓ | ✓ |
| 22/10/2024 | ITSSOC-7845 | Beast Ransomware: RaaS Platform Targets Windows, Linux, and VMware ESXi |  |  | ✓ |
| 22/10/2024 | ITSSOC-7858 | Threat Hunting Request to TI: SOC-0000427693 SOC-SPLUNK041a-Detected malware event but failed to clean from 172.31.26.183 |  |  |  |
| 23/10/2024 | ITSSOC-7861 | Attackers Target Exposed Docker Remote API Servers With 'perfctl' Malware |  |  | ✓ |
| 23/10/2024 | ITSSOC-7863 | SCAA Data Breach Attacked by Ransomware Group Trigona | ✓ | ✓ |  |
| 25/10/2024 | ITSSOC-7897 | Lumma Stealer Infects Multiple Hong Kong-Based Victims |  | ✓ |  |
| 28/10/2024 | ITSSOC-7912 | FortiManager Zero-Day Exploitation by Threat Actor Group UNC5820 (CVE-2024-47575) |  |  | ✓ |
| 29/10/2024 | ITSSOC-7937 | TeamTNT Exposed Docker Daemons |  |  | ✓ |
| 30/10/2024 | ITSSOC-7952 | Midnight Blizzard Conducts Large-Scale Spear-Phishing Campaign Using RDP Files | ✓ |  |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

In October 2024, a total of **15** threat hunting cases were handled. There were **no hits** where Indicators of Compromise (IoCs) identified through threat hunting were found within the HKMA environment.

In addition, this effort resulted in the blocking of **125** hashes, **33** domains or URLs, and **9** IP addresses. All **167** Indicators of Compromise (IoCs) were blocked, with **no IoCs** left unblocked.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Hits | Hash Blocked Count | Domain/URL Blocked Count | IP Blocked Count |
| 09/10/2024 | ITSSOC-7716 | Fake Adobe Site in Phishing Emails Targets Enterprise Networks | N/A | 14 | 17 | 1 |
| 10/10/2024 | ITSSOC-7724 | Contagious Interview Campaign Targeting Job-Seeking Individuals on LinkedIn | N/A | 38 | 0 | 0 |
| 14/10/2024 | ITSSOC-7763 | DarkVision remote access trojan (RAT): A Rising Threat in Recent Cyber Campaigns | N/A | 4 | 0 | 0 |
| 15/10/2024 | ITSSOC-7774 | Red Team Tool EDRSilencer Disrupting Endpoint Security Solutions | N/A | 1 | 0 | 0 |
| 17/10/2024 | ITSSOC-7802 | LockBit Ransomware Abuses AWS for Attack | N/A | 39 | 0 | 0 |
| 18/10/2024 | ITSSOC-7806 | Horus FUD (Fully Un-Detectable) Crypter Malware Distributor for Various Threats | N/A | 3 | 0 | 0 |
| 21/10/2024 | ITSSOC-7819 | Social Engineering via CAPTCHA Validations: Exploiting Windows Keyboard Shortcuts Could Lead User to Trigger Malicious Commands | N/A | 2 | 0 | 0 |
| 22/10/2024 | ITSSOC-7845 | Beast Ransomware: RaaS Platform Targets Windows, Linux, and VMware ESXi | N/A | 5 | 0 | 0 |
| 22/10/2024 | ITSSOC-7858 | Threat Hunting Request to TI: SOC-0000427693 SOC-SPLUNK041a-Detected malware event but failed to clean from 172.31.26.183 | N/A | 0 | 0 | 0 |
| 23/10/2024 | ITSSOC-7861 | Attackers Target Exposed Docker Remote API Servers With 'perfctl' Malware | N/A | 2 | 3 | 2 |
| 23/10/2024 | ITSSOC-7863 | SCAA Data Breach Attacked by Ransomware Group Trigona | N/A | 9 | 0 | 0 |
| 25/10/2024 | ITSSOC-7897 | Lumma Stealer Infects Multiple Hong Kong-Based Victims | N/A | 2 | 2 | 0 |
| 28/10/2024 | ITSSOC-7912 | FortiManager Zero-Day Exploitation by Threat Actor Group UNC5820 (CVE-2024-47575) | N/A | 0 | 0 | 4 |
| 29/10/2024 | ITSSOC-7937 | TeamTNT Exposed Docker Daemons | N/A | 6 | 6 | 2 |
| 30/10/2024 | ITSSOC-7952 | Government Targeted: Midnight Blizzard Conducts Large-Scale Spear-Phishing Campaign Using RDP Files | N/A | 0 | 5 | 0 |
| Total | | | | 125 | 33 | 9 |

# Phishing Email Alert Handling

## 14.1 Communications Division

There were 23 emails reported by the Communications Division that were handled in October, 2024.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 30/10/2024 | ITSPEIR-3492 | Phishing |
| 29/10/2024 | ITSPEIR-3490 | Spam |
| 28/10/2024 | ITSPEIR-3488 | Spam |
| 25/10/2024 | ITSPEIR-3486 | Spam |
| 23/10/2024 | ITSPEIR-3483 | Spam |
| 23/10/2024 | ITSPEIR-3481 | Spam |
| 22/10/2024 | ITSPEIR-3479 | Phishing |
| 21/10/2024 | ITSPEIR-3477 | Spam |
| 18/10/2024 | ITSPEIR-3475 | Phishing |
| 18/10/2024 | ITSPEIR-3473 | Phishing |
| 17/10/2024 | ITSPEIR-3469 | Phishing |
| 16/10/2024 | ITSPEIR-3463 | Phishing |
| 16/10/2024 | ITSPEIR-3461 | Phishing |
| 16/10/2024 | ITSPEIR-3460 | Phishing |
| 15/10/2024 | ITSPEIR-3458 | Spam |
| 15/10/2024 | ITSPEIR-3456 | Spam |
| 14/10/2024 | ITSPEIR-3454 | Phishing |
| 14/10/2024 | ITSPEIR-3453 | Phishing |
| 14/10/2024 | ITSPEIR-3452 | Phishing |
| 14/10/2024 | ITSPEIR-3450 | Spam |
| 09/10/2024 | ITSPEIR-3448 | Phishing |
| 02/10/2024 | ITSPEIR-3434 | Spam |
| 02/10/2024 | ITSPEIR-3432 | Spam |
| Total emails reported | | 23 |

## 14.2 Settlement Division

There were 6 emails reported by the Settlement Division that were handled in October, 2024.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 30/10/2024 | ITSPEIR-3494 | Phishing |
| 18/10/2024 | ITSPEIR-3471 | Spam |
| 08/10/2024 | ITSPEIR-3446 | Unwanted |
| 08/10/2024 | ITSPEIR-3445 | Unwanted |
| 08/10/2024 | ITSPEIR-3443 | Spam |
| 07/10/2024 | ITSPEIR-3438 | Spam |
| Total emails reported | | 6 |

## 14.3 Overview

Below is the overview of emails reported that were handled in October, 2024.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unwanted | Spam | Phishing |
| Communications Division | 0 | 11 | 12 |
| Settlements Division | 2 | 3 | 1 |
| Total emails reported | 2 | 14 | 13 |