# 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 November 2024, there were **1** high-security-level Common Vulnerabilities and Exposures (CVE), **7** medium-security-level CVE, and **1** low-security-level CVE.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Severity Level | Source | Created | Jira Ticket No. | CVE Identifier | Summary | User Confirm Affected |
| High | PwC, OGCIO, CISA | 15/11/2024 | ITSSOC-8114 | CVE-2024-0012 CVE-2024-9474 | Actively Exploited Unauthenticated Remote Command Execution Vulnerability in Palo Alto PAN-OS Management Interface | N/A |
| Medium | GovCERT.HK, PwC | 07/11/2024 | ITSSOC-8030 | CVE-2024-44258 | Apple iOS System File Modification Via Malicious Backup | MDM Admins asked for patching’s proper version |
| Medium | PwC | 07/11/2024 | ITSSOC-8032 | TBD | Veritas NetBackup on Windows Privilege Escalation Vulnerability | N/A |
| Medium | PwC | 07/11/2024 | ITSSOC-8035 | CVE-2024-42509 | HPE Aruba Networking Access Points Unauthenticated Arbitrary Command Execution Vulnerability | N/A |
| Medium | PwC. OGCIO | 13/11/2024 | ITSSOC-8082 | CVE-2024-43451  CVE-2024-49039 | Multiple Vulnerabilities in Microsoft Products November 2024 | N/A |
| Medium | PwC, OGCIO | 19/11/2024 | ITSSOC-8141 | CVE-2024-44308  CVE-2024-44309 | Multiple Vulnerabilities in Apple Products | N/A |
| Medium | PwC | 25/11/2024 | ITSSOC-8164 | CVE-2024-10979 | Postgresql Pl/Perl Environment Unauthenticated Variable Changes Execute Arbitrary Code | N/A |
| Medium | PwC | 26/11/2024 | ITSSOC-8216 | CVE-2024-5921 | PoC Released for Palo Alto Networks GlobalProtect App Insufficient Certificate Validation Leads to Privilege Escalation | N/A |
| Low | PwC | 27/11/2024 | ITSSOC-8242 | CVE-2024-10220 | Kubernetes Specially Crafted gitRepo Volumes Allow Arbitrary Command Execution | N/A |

## 12.2 Follow-up on High Severity Level CVEs

There were 1 High Severity Level CVEs Affected HKMA in November 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-2024-0012  CVE-2024-9474 | PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1, PAN-OS 11.2 | No |  | 1) Our PA firewall management interfaces are in internal management subnet, and are restricted to designated IP addresses only.  2) PA’s attack service management's also confirmed our firewall mgt is not published to Internet. |  | Justification |

## 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 November 2024.

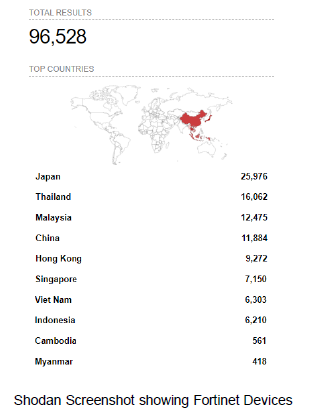
**Impact and Analysis**

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 November 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 November 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 November 2024, a total of **12** threat hunting cases were handled. These included **7** government-targeted cases, **8** APAC-targeted cases, and **5** technology-related cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Created | Jira Ticket No. | Summary | Government Targeted | APAC Targeted | Technology Related |
| 01/11/2024 | ITSSOC-7973 | Actively Exploited Microsoft SharePoint Server Gain Domain Access (CVE-2024-38094) |  |  | ✓ |
| 04/11/2024 | ITSSOC-7992 | EDR Bypass Tool Allows Threat Actor Unauthorized Data Exfiltration |  |  | ✓ |
| 06/11/2024 | ITSSOC-8014 | Orchestrated Cyber-Espionage Campaign Leads to Sensitive Information Disclosure | ✓ | ✓ |  |
| 08/11/2024 | ITSSOC-8048 | SteelFox Trojan Mimics Software Activators Stealing Sensitive Data |  | ✓ |  |
| 11/11/2024 | ITSSOC-8055 | New OceanLotus Group Delivers Trojan via MST Files for the First Time | ✓ |  |  |
| 14/11/2024 | ITSSOC-8100 | Lazarus Group’s New macOS Malware Evades Antivirus | ✓ | ✓ | ✓ |
| 18/11/2024 | ITSSOC-8134 | PXA Stealer Targets Governments Across Europe and Asia | ✓ | ✓ |  |
| 19/11/2024 | ITSSOC-8149 | New Backdoor Variant Targets Red Hat Enterprise Linux (RHEL) |  | ✓ | ✓ |
| 22/11/2024 | ITSSOC-8186 | Actively Exploited Palo Alto Networks PAN-OS Management Interface Authentication Bypass and Privilege Escalation Vulnerabilities |  |  | ✓ |
| 25/11/2024 | ITSSOC-8218 | New LODEINFO Malware Hits Government and High-Tech Across Asia | ✓ | ✓ |  |
| 28/11/2024 | ITSSOC-8251 | ANEL Backdoor Reactivated in Earth Kasha Cyber-Espionage Campaign | ✓ | ✓ |  |
| 29/11/2024 | ITSSOC-8257 | Earth Estries Chinese APT Group Exploits VPNs & Servers | ✓ | ✓ |  |

## 13.2 Indicators of Compromise (IOCs) Blocked

In November 2024, a total of **12** threat hunting cases were handled. There was **1 false positive hit** where Indicators of Compromise (IoCs) identified through threat hunting were found within the HKMA environment.

In addition, this effort resulted in the blocking of **80** hashes, **42** domains or URLs, and **24** IP addresses. All **146** 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 |
| 01/11/2024 | ITSSOC-7973 | Actively Exploited Microsoft SharePoint Server Gain Domain Access (CVE-2024-38094) | False Positive | 1 | 0 | 0 |
| 04/11/2024 | ITSSOC-7992 | EDR Bypass Tool Allows Threat Actor Unauthorized Data Exfiltration | N/A | 8 | 0 | 0 |
| 06/11/2024 | ITSSOC-8014 | Orchestrated Cyber-Espionage Campaign Leads to Sensitive Information Disclosure | N/A | 7 | 0 | 0 |
| 08/11/2024 | ITSSOC-8048 | SteelFox Trojan Mimics Software Activators Stealing Sensitive Data | N/A | 4 | 0 | 0 |
| 11/11/2024 | ITSSOC-8055 | New OceanLotus Group Delivers Trojan via MST Files for the First Time | N/A | 1 | 0 | 0 |
| 14/11/2024 | ITSSOC-8100 | Lazarus Group’s New macOS Malware Evades Antivirus | N/A | 10 | 3 | 2 |
| 18/11/2024 | ITSSOC-8134 | PXA Stealer Targets Governments Across Europe and Asia | N/A | 7 | 18 | 0 |
| 19/11/2024 | ITSSOC-8149 | New Backdoor Variant Targets Red Hat Enterprise Linux (RHEL) | N/A | 2 | 2 | 0 |
| 22/11/2024 | ITSSOC-8186 | Actively Exploited Palo Alto Networks PAN-OS Management Interface Authentication Bypass and Privilege Escalation Vulnerabilities | N/A | 22 | 0 | 0 |
| 25/11/2024 | ITSSOC-8218 | New LODEINFO Malware Hits Government and High-Tech Across Asia | N/A | 3 | 3 | 1 |
| 28/11/2024 | ITSSOC-8251 | ANEL Backdoor Reactivated in Earth Kasha Cyber-Espionage Campaign | N/A | 5 | 0 | 0 |
| 29/11/2024 | ITSSOC-8257 | Earth Estries Chinese APT Group Exploits VPNs & Servers | N/A | 6 | 16 | 21 |
| Total | | | | 80 | 42 | 24 |

Overview of False Positive Hit Case Handling (ITSSOC-7973)

Findings

One of the IoCs "98683c358724eda64bd5c1df5df6d2af8bcedd15” was identified as the hash for **adexplorer64.exe**. Checked in Sentinel 1, this file was executed by 5 users from the DO team and 4 users from the ITS team.

Justifications

ADExplorer.exe is a sophisticated Active Directory (AD) viewer and editor created by Microsoft Sysinternals, a trusted source for system utilities. This software is widely recognized as legitimate and is extensively used by IT professionals for AD management and troubleshooting.

Furthermore, TI has verified that the hash in question is a **false positive**. This means that while the hash initially triggered security alerts, upon further investigation, it was determined not to pose a threat.

Comment by AD(IT)(ITS)3

As requested by AD(IT)(ITS)3, users of ADExplorer should seek non-OA approval to use this tool. Without this approval, the use of the tool is not permitted.

Follow-up Actions

TI has notified the has notified ADExplorer users via email about the proper usage of ADExplorer, including the users of ADExplorer should seek non-OA approval to use this tool.

# Phishing Email Alert Handling

## 14.1 Communications Division

There were **27** emails reported by the Communications Division that were handled in November, 2024.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 04/11/2024 | ITSPEIR-3500 | Spam |
| 07/11/2024 | ITSPEIR-3509 | Phishing |
| 07/11/2024 | ITSPEIR-3511 | Phishing |
| 11/11/2024 | ITSPEIR-3513 | Spam |
| 15/11/2024 | ITSPEIR-3521 | Spam |
| 18/11/2024 | ITSPEIR-3523 | Phishing |
| 18/11/2024 | ITSPEIR-3525 | Phishing |
| 19/11/2024 | ITSPEIR-3527 | Unwanted |
| 19/11/2024 | ITSPEIR-3528 | Phishing |
| 19/11/2024 | ITSPEIR-3530 | Spam |
| 20/11/2024 | ITSPEIR-3532 | Spam |
| 20/11/2024 | ITSPEIR-3534 | Phishing |
| 21/11/2024 | ITSPEIR-3540 | Spam |
| 21/11/2024 | ITSPEIR-3541 | Spam |
| 21/11/2024 | ITSPEIR-3542 | Spam |
| 22/11/2024 | ITSPEIR-3546 | Phishing |
| 25/11/2024 | ITSPEIR-3548 | Phishing |
| 26/11/2024 | ITSPEIR-3550 | Phishing |
| 26/11/2024 | ITSPEIR-3552 | Spam |
| 26/11/2024 | ITSPEIR-3554 | Phishing |
| 26/11/2024 | ITSPEIR-3555 | Phishing |
| 26/11/2024 | ITSPEIR-3557 | Phishing |
| 27/11/2024 | ITSPEIR-3558 | Spam |
| 27/11/2024 | ITSPEIR-3560 | Spam |
| 27/11/2024 | ITSPEIR-3561 | Spam |
| 28/11/2024 | ITSPEIR-3563 | Spam |
| 29/11/2024 | ITSPEIR-3566 | Spam |
| Total emails reported | | 27 |

## 14.2 Settlement Division

There were **4** emails reported by the Settlement Division that were handled in November, 2024.

|  |  |  |
| --- | --- | --- |
| Created | Jira Ticket No. | Category |
| 05/11/2024 | ITSPEIR-3502 | Spam |
| 06/11/2024 | ITSPEIR-3504 | Spam |
| 06/11/2024 | ITSPEIR-3505 | Spam |
| 11/11/2024 | ITSPEIR-3515 | Spam |
| Total emails reported | | 4 |

## 14.3 Overview

In November, 2024, TI has acknowledged **31** suspicious email reports by users, confirming that there are **1** unwanted emails, **17** spam emails, and **13** 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.

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unwanted | Spam | Phishing |
| Communications Division | 1 | 13 | 13 |
| Settlements Division | 0 | 4 | 0 |
| Total emails reported | 1 | 17 | 13 |