# Threat Intelligence

## SOP Status of Operational Intelligence in October (Until 25th Oct)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Content of SOP | Detail | Stage | Status | Responsible Person |
| Cyber Threat Operations (CTO) | Modification of 4th Draft (Updated on 5 Nov)  1) High / Critical Case  - Add a step “Email to System Owner confirm if system is affected” before routing JIRA sub-ticket to System Owner  - TI on-site analyst creates sub-ticket to fill in the response from System Owner’s email reply, instead of System Owner creating sub-ticket and filling in the information themselves  - Set the component of JIRA sub-ticket to “TI follow up” instead of “TI alert escalation”  2) Add Case Categorization – align OGCIO - Threat Handling Guideline  - Social threats  - Technical Threats  - Environmental Threats  - Others (e.g., Threat Landscape) | Kick started on beginning of June | PwC updated SOP on Sep and is pending on confirmation by HKMA | PwC, HKMA |
| Security Operations Centre (SOC) | Modification of 2nd Draft (Updated on 5 Nov)  1) Add “SOC create and route sub-ticket to TI on-site analyst for Threat Hunting” if malware is found in the HKMA system | Kick started on beginning of June | PwC sent out SOP on Aug and is pending on confirmation by HKMA | PwC, HKMA |
| Threat Hunting | Modification of 1st Draft (Updated on 5 Nov)  1) Remove Session 2.6 - Review and Consolidation HKMA Internal TI Source is removed - the IOC consolidation is inefficient after trial run, we proposed to remove this part due to no any integration in place, there is no impact on current threat hunting tasks. | Kick started on beginning of Aug | PwC sent out SOP on Aug and is pending on confirmation by HKMA | PwC, HKMA |
| Incident Response (IR) | Last Modification of 1st Draft (in Aug) | On Demand | PwC sent out SOP on Aug and is pending on confirmation by HKMA | PwC, HKMA |

## 

## Major Threat Intelligence Report Highlight

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

1. Multiple Palo Alto Networks Expedition Vulnerabilities Lead to Exposure of Firewall Credentials
2. PoC Released Use After Free Vulnerability in Adobe Reader and Acrobat (CVE-2024-41869)

Executive Summary

|  |  |
| --- | --- |
| Threat Intelligence | TI/SOC Recommendation/Actionable Item |
| 1. Multiple Palo Alto Networks Expedition Vulnerabilities Lead to Exposure of Firewall Credentials | * Send an outlook email to notify potentially affected parties to apply the patch |
| 1. Actively Exploited Fortinet Multiple Products Format String Bug Allows Critical RCE Vulnerability, PoC Released (CVE-2024-23113) | * Send an outlook email to notify potentially affected parties to apply the patch |

### 1. Multiple Palo Alto Networks Expedition Vulnerabilities Lead to Exposure of Firewall Credentials

On 10 October 2024, Palo Alto Networks Security Advisories disclosed multiple vulnerabilities in Palo Alto Networks Expedition.1 Successful exploitation could lead to the takeover of firewall admin accounts, exposing sensitive information such as usernames, cleartext passwords, and API keys for PAN-OS firewalls. In addition, we note that the proof-of-concept (PoC) code for the vulnerabilities CVE-2024-9464 and CVE-2024-9465 is publicly available.

**Impact and Analysis**

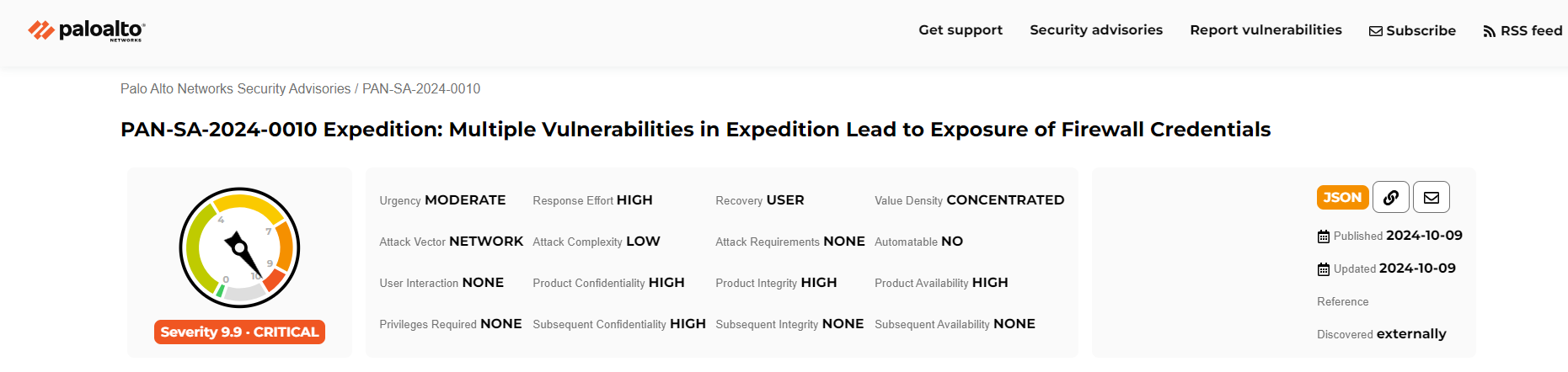
CVE-2024-9464 is a similar OS command injection vulnerability comparing with CVE-2024-9463, but requiring authentication, allowing attackers to exploit Expedition and run OS commands as root. Additionally, a proof-of-concept to exploit CVE-2024-9464 is publicly available, enabling arbitrary command execution.

CVE-2024-9465 is an SQL injection vulnerability allowing unauthorized attackers to access Expedition’s database, revealing password hashes, usernames, and more. Additionally, a proof-of-concept to exploit CVE-2024-9465 is publicly available, enabling SQL Injection.

PwC’s Dark Lab strongly urges impacted clients to apply the patch as soon as possible to remediate risk. This is particularly given the presence of proof-of-concept vulnerabilities, and multiple highly sensitive information disclosure vulnerabilities, which could lead to account takeover via obtained credentials.

Affected Products:

* Expedition < 1.2.96



### 2. Actively Exploited Fortinet Multiple Products Format String Bug Allows Critical RCE Vulnerability, PoC Released (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.

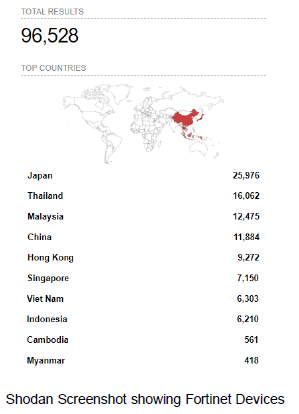
The Proof-of-Concept (PoC) was released on March 2024, whilst it has been recently listed on CISA’s Known Exploited Vulnerabilities Catalog on 9 October 2024.

**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 last week, the CISA raised confirmed that CVE-2024-23113 has been actively being exploited in the wild. Research indicates that thousands of Fortinet devices remain exposed, posing a significant risk to critical infrastructure, businesses, and government organizations. The vulnerability requires minimal effort to exploit, making it particularly dangerous.

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 7.0 – 7.0.13
* FortiOS 7.2.0 – 7.2.6
* FortiOS 7.4.0 – 7.4.2
* FortiPAM 1.0, 1.1, and 1.2 – all versions
* FortiProxy 7.0.0 – 7.0.15
* FortiProxy 7.2.0 – 7.2.8
* FortiProxy 7.4.0 – 7.4.2
* FortiWeb 7.4.0 – 7.4.2

## Threat Intelligence Report List in October

|  |  |  |  |
| --- | --- | --- | --- |
| Created | Issue key | Summary | Email Notification to impacted parties? |
| 30/09/2024 | ITSSOC-7624 | [TI] [CVE] [Wordpress GiveWP plugin] CVE-2024-8353 (CVSS 10): Critical GiveWP Flaw |  |
| 30/09/2024 | ITSSOC-7622 | [TI] [CVE] [Zimbra] Zimbra - Remote Command Execution (CVE-2024-45519) | ✓ |
| 30/09/2024 | ITSSOC-7618 | [TI] [CVE] [NVIDIA Container Toolkit] CVE-2024-0132 container escape attacks and gain full access to the host system |  |
| 26/09/2024 | ITSSOC-7567 | [TI] [CVE] [Aruba] Aruba Access Points Exposes to Remote Code Execution (RCE) Attacks (CVE-2024-42505, CVE-2024-42506, CVE-2024-42507) |  |
| 26/09/2024 | ITSSOC-7562 | [TI] [CVE] [FlashArray] FlashArray Purity Exposed Local Configuration Account Vulnerability (CVSS: 10) | ✓ |
| 24/09/2024 | ITSSOC-7533 | [TI] [CVE] [Grafana] Critical Grafana Plugin SDK Flaw Exposes Sensitive Information (CVE-2024-8986) | ✓ |
| 23/09/2024 | ITSSOC-7514 | [TI] [CrowdStrike] CrowdStrike Outage Disrupts Global Financial Sector and Central Banks |  |
| 20/09/2024 | ITSSOC-7503 | [OGCIO] [TI] [CVE] High Threat Security Alert (A24-09-16): Multiple Vulnerabilities in VMware Products | ✓ |
| 20/09/2024 | ITSSOC-7502 | [OGCIO] [TI] [CVE] High Threat Security Alert (A24-09-17): Vulnerability in GitLab for subscribers (CVE-2024-45409) | ✓ |
| 16/09/2024 | ITSSOC-7448 | [OGCIO] [TI] [CVE] High Threat Security Alert (A24-09-08): Multiple Vulnerabilities in Microsoft Products (September 2024) | ✓ |
| 16/09/2024 | ITSSOC-7447 | [OGCIO] [TI] [CVE] High Threat Security Alert (A24-09-09): Multiple Vulnerabilities in Ivanti Products |  |
| 16/09/2024 | ITSSOC-7446 | [OGCIO] [TI] [CVE] Further Update to High Threat Security Alert (A24-09-11a): Multiple Vulnerabilities in Adobe Reader/Acrobat | ✓ |
| 16/09/2024 | ITSSOC-7439 | [TI] [CVE] [Palo Alto] Command Injection Vulnerability in Palo Alto Networks PAN-OS (CVE-2024-8686) | ✓ |
| 16/09/2024 | ITSSOC-7438 | [OGCIO] [TI] [CVE] High Threat Security Alert (A24-09-14): Multiple Vulnerabilities in GitLab | ✓ |
| 16/09/2024 | ITSSOC-7437 | [TI] [CVE] [Kibana] Kibana?s Amazon Bedrock Connector Deserialization Flaw Lead to Remote Code Execution [CVE-2024-37288] | ✓ |
| 16/09/2024 | ITSSOC-7435 | [TI] [CVE] [Jenkins] [PoC Available] PoC released for Critical Jenkins Vulnerability Exposes Servers to RCE Attacks (CVE-2024-43044) | ✓ |
| 09/09/2024 | ITSSOC-7362 | [OGCIO] [TI] [CVE] Further Update to High Threat Security Alert (A24-08-13a): Vulnerability in SonicWall Products for subscribers |  |
| 06/09/2024 | ITSSOC-7347 | [TI] [CVE] [Veeam] Veeam Backup & Replication Faces RCE Flaw Allows Full System Takeover [CVE-2024-40711, CVSS v3: 9.8] | ✓ |