Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Versa Networks Patches Severe Zero-Day Flaw in Director Software

Date of Publication	Last updated date	Admiralty Code	TA Number
August 27, 2024	August 28, 2024	A2	TA2024329

Summary

First Seen: June 12, 2024
Affected Product: Versa Director
Malware: VersaMem
Threat Actor: Volt Typhoon (also known as Vanguard Panda, Bronze Silhouette, Dev-0391, UNC3236, Voltzite, and Insidious Taurus)
Impact: A high-severity vulnerability (CVE-2024-39717) in Versa Director allows malicious file uploads by users with certain admin privileges, primarily due to a lack of implemented system hardening and firewall guidelines. Exploited by the Chinese APT group Volt Typhoon, it has led to the deployment of a web shell for credential harvesting. Versa has released patches and urges customers to apply these updates and follow security best practices.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-39717	Versa Director Dangerous File Type Upload Vulnerability	Versa Director	✓	✓	✓

Vulnerability Details

#1 CVE-2024-39717 is a significant vulnerability affecting the Versa Director platform, widely used by managed service providers (MSPs) for the management and orchestration of Secure Access Service Edge (SASE) services. This vulnerability stems from an unrestricted file upload flaw in the "Change Favicon" feature of the Versa Director GUI.

#2 The flaw allows authenticated users with specific administrative privileges (Provider-Data-Center-Admin or Provider-Data-Center-System-Admin) to upload potentially malicious files disguised as PNG images. Although the vulnerability has a CVSS score of 7.2, indicating high severity, its impact can be severe if exploited.

#3 The vulnerability has been actively exploited in the wild. Reports confirm that an Advanced Persistent Threat (APT) actor, specifically the Chinese state-sponsored group Volt Typhoon, exploiting this vulnerability. These attackers have deployed a custom web shell named "VersaMem" to harvest credentials and gain further access to compromised networks. Their activities have primarily targeted downstream customers of ISPs and MSPs, indicating a broader risk to organizations relying on these services.

#4 The exploitation typically occurs when customers do not implement recommended system hardening and firewall guidelines, which leads to exposed management ports. Attackers can then gain initial access and execute malicious files on the server, significantly threatening affected systems.

#5 In response, Versa Networks has released patches and strongly advised to upgrade to the latest version of Versa Director. It’s important to adhere to the established firewall guidelines and system hardening practices of Versa, which have been available since 2015 and 2017. Organizations are urged to inspect their environments for any signs of exploitation, particularly by checking specific directories for suspicious files that may have been uploaded.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-39717	Versa Director: 21.2.3 Versa Director: 22.1.2 Versa Director: 22.1.3	cpe:2.3:a:versa-networks:versa_director:*:*:*:*:*:*:*:*	CWE-434

Recommendations

Apply Patches Immediately: Ensure that the latest security patches released by Versa Networks are applied to the Versa Director platform. This is critical to close the vulnerability and prevent exploitation. After applying the patches, verify that the updates have been correctly installed and are functioning as intended.

Check for Evidence of Exploitation: Examine the /var/versa/vnms/web/custom_logo/ directory for any suspicious files. Use the file -b --mime-type <.png file> command to verify that files are legitimate (should report as "image/png").

Secure Management Ports: Ensure that management ports are not exposed to the public internet. Limit access to these ports by using firewalls, VPNs, or IP whitelisting to allow only trusted networks or devices to connect, reducing the risk of unauthorized access and exploitation.

Implement System Hardening: Adhere strictly to Versa's published system hardening guidelines, which include disabling unnecessary services, securing management ports, and applying the least privilege principle. Ensure that only essential ports and protocols are open as per the Firewall Requirements established by Versa since 2015.

Enhance Upload Security: Ensure that all file uploads are subject to strict validation checks. This includes verifying file types, sizes, and contents to prevent malicious files from being uploaded. Deploy a WAF to monitor and filter incoming traffic, which can help detect and block attempts to exploit vulnerabilities in web applications.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0001 Initial Access	TA0003 Persistence	TA0043 Reconnaissance	TA0011 Command and Control
T1190 Exploit Public-Facing Application	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1036.008 Masquerade File Type

T1036 Masquerading	T1068 Exploitation for Privilege Escalation	T1588.005 Exploits	T1106 Native API
T1059 Command and Scripting Interpreter	T1136 Create Account	T1027 Obfuscated Files or Information	T1055 Process Injection
T1505.003 Web Shell	T1505 Server Software Component	T1589.001 Credentials	T1589 Gather Victim Identity Information
T1071 Application Layer Protocol	T1571 Non-Standard Port		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37
File Path	/tmp/[.]temp[.]data

Patch Details

Upgrade Versa Director to version 22.1.4 or later. Please refer to the links below for versions 21.2.3, 22.1.2, and 22.1.3.

Links:
https://support.versa-networks.com/support/solutions/articles/23000024323-release-21-2-3

https://support.versa-networks.com/support/solutions/articles/23000025680-release-22-1-2

https://support.versa-networks.com/support/solutions/articles/23000026033-release-22-1-3

References

https://versa-networks.com/blog/versa-security-bulletin-update-on-cve-2024-39717-versa-director-dangerous-file-type-upload-vulnerability/

https://www.securityweek.com/chinese-apt-volt-typhoon-caught-exploiting-versa-networks-sd-wan-zero-day/

https://www.cisa.gov/news-events/alerts/2024/08/27/versa-networks-releases-advisory-vulnerability-versa-director-cve-2024-39717

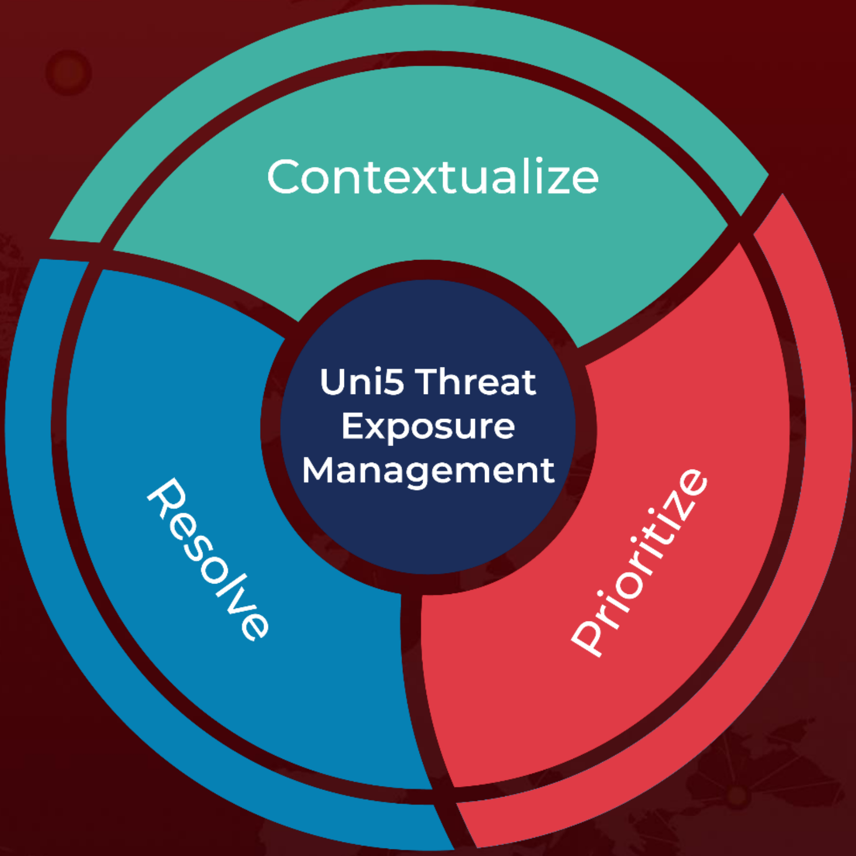
https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

https://www.hivepro.com/threat-advisory/volt-typhoon-a-cyber-threat-to-u-s-critical-infrastructure/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 27, 2024 • 5:30 AM

More at www.hivepro.com