Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2024-41992: Unpatched Zero-Day RCE Flaw Found in Arcadyan Routers

Date of Publication	Admiralty Code	TA Number
August 23, 2024	A1	TA2024325

Summary

First Seen: April 2024
Affected Product: Arcadyan routers
Impact: CVE-2024-41992 is a severe zero-day vulnerability in the Arcadyan FMIMG51AX000J and potentially other WiFi Alliance devices using the same firmware, allowing remote code execution. The flaw stems from a test utility service on ports 8000 and 8080, which mishandles TLV packets, enabling command injection. A proof-of-concept exploit has been released, and despite being reported in April 2024, no fix is available. Users are advised to restrict remote access and isolate affected devices until a patch is provided.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-41992	Arcadyan Remote Code Execution Vulnerability	Arcadyan routers	✓	✗	✗

Vulnerability Details

#1 CVE-2024-41992 is a critical zero-day vulnerability found in the DUT-Wi-FiTestSuite-9.0.0 impacting Arcadyan FMIMG51AX000J model and potentially other WiFi Alliance-affiliated devices employing the DUT-Wi-FiTestSuite. This vulnerability allows remote attackers to execute arbitrary code, potentially gaining full control over the affected devices. This could enable attackers to manipulate network traffic, intercept sensitive data, or launch additional attacks on connected systems.

#2 The vulnerability arises from a test utility service running on the device, which listens on ports 8000 and 8080. This service, intended for device testing during development, improperly handles input, making it susceptible to command injection attacks.

#3

Technical analysis reveals that the vulnerability is linked to how the service processes TLV (Type-Length-Value) packets. When a TLV packet is sent to the service, the parameters are parsed and used in command execution. Certain functions within the service, particularly the wfaTGSendPing function, accept larger inputs, providing an avenue for broader exploitation. This makes it possible for attackers to inject and execute commands on the affected device remotely.

#4

A proof-of-concept (PoC) exploit for this vulnerability has already been publicly released, increasing the risk of exploitation. The issue was first reported in April 2024, but as of now, there has been no fix from the vendor or the WiFi Alliance. Users are advised to restrict remote access, monitor network traffic, and segregate vulnerable devices from critical networks as temporary mitigation steps until a patch is available.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-41992	Arcadyan FMIMG51AX000J DUT-Wi-FiTestSuite-9.0.0	cpe:2.3:o:arcadyan:fmimg5ax000j_firmware:*:*:*:*:*:*:*:*	CWE-20

Recommendations

Monitor for Updates and Patches: Closely monitor for any security updates or patches released by Arcadyan or the Wi-Fi Alliance for the affected FMIMG51AX000J model. Apply any available patches as soon as possible to mitigate the risks associated with this vulnerability.

Restrict Remote Access: Disable or limit remote access to the affected devices by blocking access to ports 8000 and 8080 from external networks. Implement strong authentication measures, such as multi-factor authentication, to prevent unauthorized access.

Network Segmentation: Isolate vulnerable devices from critical networks and systems to prevent potential lateral movement by attackers.

Monitor Network Traffic: Implement monitoring tools to detect unusual or suspicious activity, particularly on the affected ports, to identify and respond to potential exploits.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	T1588.006 Vulnerabilities	T1588.005 Exploits
T1203 Exploitation for Client Execution	T1588 Obtain Capabilities	T1059 Command and Scripting Interpreter	

Patch Details

As of now, no patch has been released to address CVE-2024-41992.

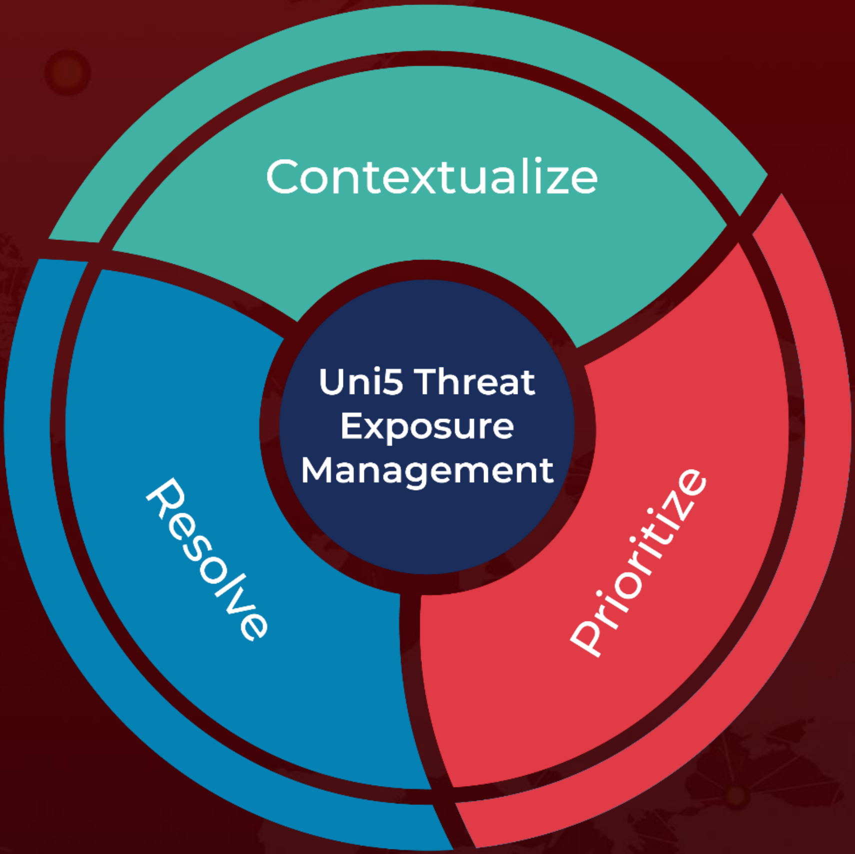
References

https://ssd-disclosure.com/ssd-advisory-arcadyan-fmimg51ax000j-wifi-alliance-rce/

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 23, 2024 • 5:30 AM

More at www.hivepro.com