Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Flaw in Microchip ASF Exposes Devices to Remote Code Execution

Date of Publication	Admiralty Code	TA Number
September 26, 2024	A1	TA2024373

Summary

First Seen: August 2024
Affected Products: Microchip Advanced Software Framework (ASF)
Impact: A critical vulnerability, CVE-2024-7490, has been discovered in the Microchip Advanced Software Framework (ASF), which could lead to remote code execution. This flaw is due to a stack-based buffer overflow in ASF's tinydhcp server caused by insufficient input validation. Successful exploitation leads to memory corruption and potential arbitrary code execution on the affected system. Users should replace the vulnerable DHCP component immediately, as the vendor no longer supports the software.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-7490	Microchip Advanced Software Framework (ASF) Improper Input Validation Vulnerability	Microchip Advanced Software Framework (ASF)	❌	❌	❌

Vulnerability Details

#1

A critical vulnerability has been uncovered in the Microchip Advanced Software Framework (ASF), potentially leading to remote code execution (RCE). Tracked as CVE-2024-7490, this flaw is rated with a high severity, carrying a CVSS score of 9.5/10. The vulnerability stems from a stack-based buffer overflow in ASF's tinydhcp server implementation, caused by insufficient input validation. If an attacker sends specially crafted DHCP packets, they could exploit this flaw to corrupt memory, ultimately allowing them to execute arbitrary code on the affected systems.

#2 ASF is a widely used software framework designed to make it easier for developers to build applications on Microchip microcontrollers. It includes drivers, libraries, and examples that abstract the low-level hardware, helping developers reduce the time spent on coding. However, the vulnerability in its DHCP implementation poses significant risks, especially since ASF is often found in IoT devices, making it likely to be used in many environments.

#3 The issue is present in all public examples of the ASF codebase, where a crafted DHCP request can trigger the buffer overflow. There are also forks of the tinydhcp software on GitHub that may be vulnerable, further broadening the risk. Since the vendor no longer supports the software, organizations using ASF or any of its forks should act quickly to mitigate the threat by replacing the vulnerable DHCP component.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-7490	Microchip Advanced Software Framework: through 3.52.0.2574	cpe:2.3:a:microchip:advanced_software_framework:*:*:*:*:*:*:*:*	CWE-120 CWE-20

Recommendations

Replace Service: To mitigate the risks posed by CVE-2024-7490 in the Microchip Advanced Software Framework (ASF), it is highly recommended to replace the vulnerable tinydhcp service with a more secure and well-maintained alternative. Since tinydhcp is no longer supported and suffers from a critical stack-based overflow vulnerability, continuing to use it exposes systems to remote code execution risks.

Implement Monitoring and Logging: It is crucial to implement robust logging and monitoring practices to detect potential exploitation of CVE-2024-7490 or similar vulnerabilities. Organizations should enable detailed logging for their DHCP services and monitor system logs closely for any unusual behavior, such as crashes or unexpected service restarts, which could indicate attempted exploitation.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1059 Command and Scripting Interpreter			

Patch Details

There is no fix or workaround available for CVE-2024-7490 yet. The only option is to replace the tinydhcp service with a different one that doesn’t have this vulnerability.

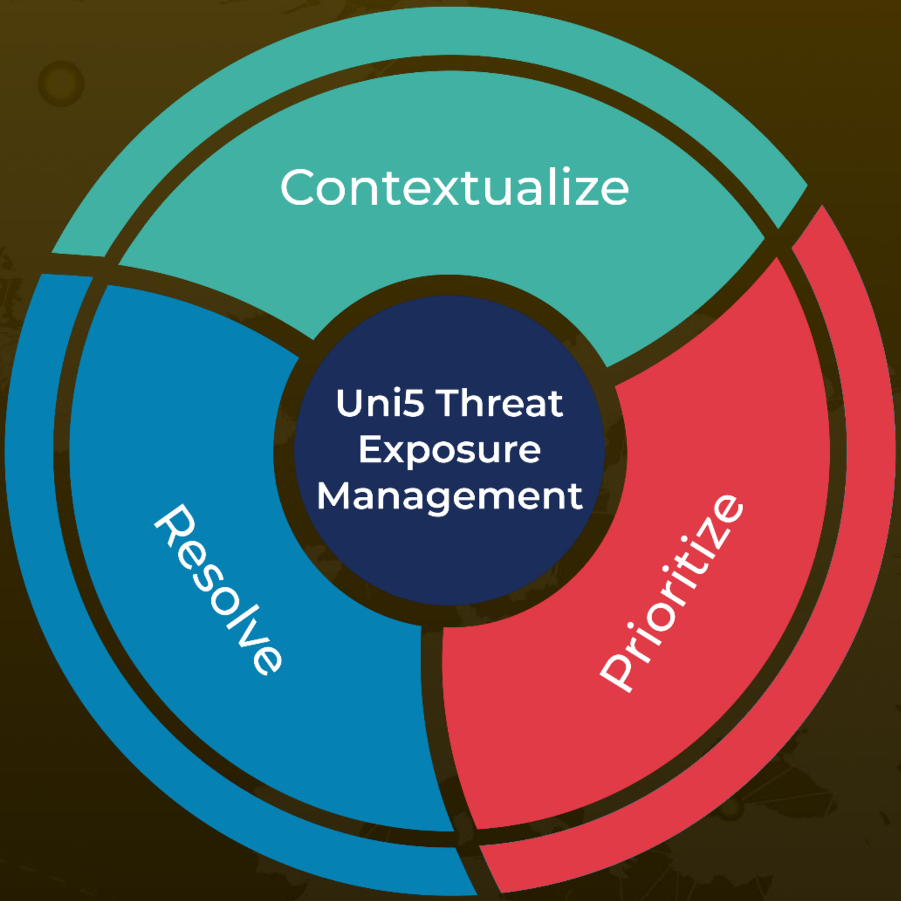
References

https://kb.cert.org/vuls/id/138043

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

September 26, 2024 • 10:10 PM

More at www.hivepro.com