مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Microchip ASF

Tracking #:432316315

Date:23-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the Microchip Advanced Software Framework (ASF) tinydhcp server, which could allow remote code execution on vulnerable IoT devices.

TECHNICAL DETAILS:

A critical vulnerability has been identified in the Microchip Advanced Software Framework (ASF) tinydhcp server, which could allow remote code execution on vulnerable IoT devices. This vulnerability, tracked as **CVE-2024-7490(CVSS-B:9.5 CRITICAL)**, poses a significant threat to the security of numerous IoT deployments.

Due to the discontinued support for ASF, no official patch is available. Organizations using ASF are strongly advised to take immediate action to mitigate the risk. The affected software is ASF 3.52.0.2574 and all prior versions.

Potential Impact:

- Remote Code Execution: Attackers can gain unauthorized access to vulnerable devices and execute malicious code, potentially leading to data breaches, service disruptions, and other severe consequences.
- Compromised IoT Devices: A large number of IoT devices are likely affected, as ASF is widely used in the IoT ecosystem.

RECOMMENDATIONS:

- Migrate to a Supported DHCP Implementation: Replace the vulnerable tinydhcp server with a more secure and actively supported DHCP implementation.
- Network Segmentation: Isolate affected devices from critical infrastructure to minimize potential damage from exploitation.
- Monitoring and Detection: Implement enhanced monitoring solutions to detect unusual network traffic patterns indicative of exploitation attempts.
- Regular Security Audits: Conduct regular security audits to identify and address other vulnerabilities in your IoT infrastructure.
- Secure Network Configuration: Implement strong network security measures, such as firewalls and intrusion detection systems, to protect against unauthorized access.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-7490