مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in Zephyr RTOS

Tracking #:432318545

Date:09-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the Zephyr RTOS affecting the DNS resolver component.

TECHNICAL DETAILS:

A critical vulnerability has been identified in the Zephyr RTOS affecting the DNS resolver component. The flaw, tracked as CVE-2026-1678, carries a CVSS v3.1 score of 9.4 and may allow unauthenticated remote attackers to execute arbitrary code on affected devices.

The vulnerability arises from improper memory boundary handling in the dns_unpack_name() function within the DNS parsing library. Attackers can exploit this flaw by sending specially crafted DNS responses that trigger an out-of-bounds memory write, potentially leading to Remote Code Execution (RCE).

Zephyr RTOS is widely used in IoT devices, embedded systems, sensors, wearables, and industrial gateways, the vulnerability may impact millions of devices globally if DNS resolver functionality is enabled.

Vulnerability Details

- **CVE ID:** CVE-2026-1678
- **Severity:** Critical
- **CVSS Score:** 9.4 (CVSS v3.1)
- **Affected Component:** DNS Resolver library in Zephyr RTOS
- **Vulnerable Function:** dns_unpack_name()
- **Attack Vector:** Network (via crafted DNS responses)
- **Authentication Required:** No
- **Impact:** Remote Code Execution (RCE), memory corruption

RECOMMENDATIONS:

1. Apply Security Updates

- Upgrade to the latest patched version of Zephyr RTOS where the DNS parsing logic has been hardened.

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://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-536f-h63g-hj42