مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

IP Spoofing Vulnerability in Zephyr RTOS

Tracking #:432315726

Date:25-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in the Zephyr Real-Time Operating System (RTOS) that could allow attackers to potentially spoof IP addresses.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2023-7060 (CVSS Score 8.6,High)**
  - Zephyr OS IP packet handling does not properly drop IP packets arriving on an external interface with a source address equal to 127.0.01 or the destination address.

Affected Products:

All unpatched releases of Zephyr OS supporting IPv6 or IPv4.

- Zephyr OS v.3.5
- Zephyr OS v.3.4
- Zephyr OS v.2.7 (LTS v2)
- And all other releases supporting IPv6 or IPv4

Remediation:

The fix is included as of the commit

- Zephyr OS main: fa0e04e2edb82bf880b274d9532fcf2729f4d674
- Zephyr OS v.3.5: 62e3c7d871852a23cb5b2dbd7c74f7d5e150f7ea
- Zephyr OS v.3.4: 339194de6e79198e86b83fba5118039974112cfa
- Zephyr OS v.2.7 (LTS v2): 01ad11252ced4cf2e4828a5b5f263cf8d631b6c2
- Patches are not cherry-picked to other releases, which remain vulnerable
- Zephyr OS v.3.6 and newer versions inherit the fix from the main repository.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Zephyr

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:

1. https://synopsys.com/blogs/software-security/cyrc-vulnerability-advisory-cve-2023-7060-missing-security-control-zephyr.html