CVE-2025-1673: DENIAL OF SERVICE IN ZEPHYR RTOS

Vairav Advisory Report

Date: 2025-02-28

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability identified as **CVE-2025-1673** has been discovered in the Zephyr Project's DNS packet handling. This flaw allows remote attackers to cause a denial-of-service (DoS) condition or incorrect computations by sending specially crafted DNS packets without a payload. The vulnerability has been assigned a **CVSS score of 8.2**, categorizing it as High severity. Exploitation of this vulnerability could lead to system crashes or erroneous data processing over **multiple industries including IoT, Consumer Electronics, Healthcare devices, networking and communication equipment and energy management systems.**

VULNERABILITY DETAILS

CVE-2025-1673

- **Description:** The vulnerability arises from an out-of-bounds read in the dns_validate_msg function within the resolve.c file of the Zephyr Project. When the system processes a malicious or malformed DNS packet lacking a payload, it can trigger this out-of-bounds read, leading to a crash or incorrect computation.
- **Impact:** Successful exploitation allows remote attackers to cause a denial-of-service by crashing the system or inducing incorrect computational results. This can disrupt services and potentially lead to further security issues.
- **CVSS Score:** 8.2 (High)

AFFECTED VERSIONS

The following versions of the Zephyr Project are affected:

- Zephyr versions up to and including 4.0

EXPLOIT DETAILS

In environments where the Zephyr Project's DNS resolver is utilized, an attacker can send specially crafted DNS packets without a payload to exploit this vulnerability. No prior authentication or user interaction is required, making it possible for remote attackers to disrupt services or cause incorrect computations, leading to potential data integrity issues.

RECOMMENDED ACTIONS

- Add a **DNS payload validation** that verifies that the **qdcount** and **amcount** values present in the header are correct.

- Patch and Upgrade to fixed versions as mentioned in Zephyr's security advisory.

ADDITIONAL SECURITY MEASURES

- **Network Filtering:** Implement network-level filtering to block malformed DNS packets from untrusted sources.
- **Intrusion Detection Systems:** Deploy intrusion detection systems to monitor and alert on suspicious DNS traffic patterns.
- **Access Controls:** Restrict access to DNS services to trusted networks and authenticated users only.
- **Regular Audits**: Conduct regular security audits and code reviews to identify and mitigate potential vulnerabilities.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-1673
- https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-jjhx-rrh4-j8mx

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com