مجلس الأمن السيبراني
# CYBER SECURITY COUNCIL
United Arab Emirates

**High-Severity Denial-of-Service Vulnerability in ISC BIND 9**
Tracking #:432318297
Date:23-01-2026

TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in ISC BIND 9 that could be exploited to cause denial-of-service (DoS) conditions across critical DNS infrastructure.

## TECHNICAL DETAILS:

A high-severity vulnerability has been identified in BIND 9 that allows a remote attacker to crash affected servers by sending a specially crafted DNS packet, potentially causing denial-of-service (DoS) conditions across critical DNS infrastructure.

**Vulnerability Details**
- **CVE-2025-13878**
- **CVSS Score:** 7.5 High
- The vulnerability resides in the named process and is caused by improper handling of malformed BRID and HHIT DNS record data structures. A single malicious DNS request containing corrupt records may cause the process to terminate unexpectedly. Both authoritative DNS servers and recursive resolvers are affected.

**Affected Products**
- BIND 9:
    - 9.18.40 -> 9.18.43
    - 9.20.13 -> 9.20.17
    - 9.21.12 -> 9.21.16
- BIND Supported Preview Edition
    - 9.18.40-S1 -> 9.18.43-S1
    - 9.20.13-S1 -> 9.20.17-S1

**Fixed Versions:**
- BIND 9:
    - BIND 9.18.44
    - BIND 9.20.18
    - BIND 9.21.17
- BIND Supported Preview Edition
    - 9.18.44-S1
    - 9.20.18-S1

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by ISC.

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://kb.isc.org/docs/cve-2025-13878