مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in ISC BIND 9

Tracking #:432318686

Date:30-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the Internet Systems Consortium has disclosed multiple vulnerabilities in BIND 9 that could lead to access control bypass, denial-of-service (DoS), and service crashes, impacting both DNS resolvers and authoritative servers.

TECHNICAL DETAILS:

Vulnerability Details

CVE-2026-3591 – ACL Bypass

- **Severity:** Medium
- A stack use-after-return vulnerability in the handling of SIG(0) signed queries may allow attackers to bypass Access Control Lists (ACLs). Specially crafted DNS requests can cause incorrect IP address matching, potentially allowing unauthorized access in default-allow configurations.

CVE-2026-1519 – CPU Resource Exhaustion (DoS)

- **Severity:** High
- This vulnerability affects DNS resolvers performing DNSSEC validation. Attackers can exploit malicious zones with excessive NSEC3 iterations, leading to high CPU consumption and degraded query performance, potentially resulting in denial-of-service conditions.

CVE-2026-3119 – TKEY Query Crash

- **Severity:** Medium
- A flaw in processing valid TKEY queries with trusted TSIG signatures may cause the BIND (named) service to terminate unexpectedly, resulting in a DNS service outage. Exploitation requires a trusted key configured on the server.

Affected Products

- BIND 9 versions:
  - 9.11.0 – 9.16.50
  - 9.18.0 – 9.18.46
  - 9.20.0 – 9.20.20
  - 9.21.0 – 9.21.19

Fixed Versions

- 9.18.47
- 9.20.21
- 9.21.20

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2026-3591
- https://kb.isc.org/docs/cve-2026-1519
- https://kb.isc.org/docs/cve-2026-3119