

ISC BIND Vulnerability Enables Denial-of-Service Attacks via TKEY Queries



A data processing vulnerability in ISC BIND allows remote attackers to trigger denial-of-service conditions through specially crafted TKEY queries.

- CVE-2015-5477 affects ISC BIND DNS server software with a data processing error
- Remote attackers can exploit the flaw via TKEY queries to cause denial of service
- Organisations should apply vendor patches and mitigations immediately
- Institutions must evaluate internet exposure of affected DNS infrastructure
- Compliance with vendor security guidance is essential for regulated entities

Vulnerability Overview

ISC BIND, a widely deployed DNS server software, contains a data processing vulnerability tracked as **CVE-2015-5477**. The flaw enables remote attackers to cause a denial-of-service condition by sending specially crafted TKEY queries to vulnerable servers. This vulnerability poses operational risks to organisations relying on BIND for domain name resolution services, particularly those in regulated sectors where service availability is critical.

The vulnerability requires no authentication and can be exploited remotely, making it an attractive target for threat actors seeking to disrupt DNS infrastructure. Successful exploitation results in service interruption, potentially affecting business continuity and access to critical systems.

Risk to Saudi Institutions

Regulated institutions in the Kingdom operating ISC BIND servers should treat this vulnerability as a priority. DNS infrastructure underpins essential services across banking, healthcare, energy and government sectors. A denial-of-service attack against DNS servers can cascade into broader service outages, affecting customer access, internal operations and regulatory reporting systems.

Organisations must assess whether their DNS infrastructure is exposed to the internet and evaluate the potential impact of service disruption on compliance obligations and operational resilience.

Remediation Guidance

Vendor patches and mitigations are available for this vulnerability. Institutions should apply updates in accordance with ISC's security advisories and their own change management procedures. Where immediate patching is not feasible, consider implementing network-level controls to restrict TKEY query processing or limit exposure of DNS servers to untrusted networks. Organisations using cloud-based DNS services should verify that their providers have addressed this vulnerability.

What to do now

1. Identify all ISC BIND servers in your environment and verify their version and patch status
2. Apply vendor-supplied patches and security updates immediately following change management procedures
3. Assess internet exposure of DNS infrastructure and document all externally accessible BIND instances
4. Implement network controls to restrict TKEY query processing or limit DNS server exposure where patching is delayed
5. Verify that cloud DNS service providers have addressed CVE-2015-5477 in their infrastructure
6. Review DNS service availability monitoring and incident response procedures for denial-of-service scenarios