مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Multiple vulnerabilities in BIND 9 DNS software

Tracking #:432316090
Date:26-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities in BIND 9 DNS software could be exploited for denial-of-service (DoS) attacks.

TECHNICAL DETAILS:

The Internet Systems Consortium (ISC) has released patches to address multiple security vulnerabilities in BIND 9 DNS software could be exploited for denial-of-service (DoS) attacks.

- **CVE-2024-4076**: Logic error leading to assertion failure (CVSS 7.5).
- **CVE-2024-1975**: Excessive CPU load during DNS message validation (CVSS 7.5).
- **CVE-2024-1737**: Potential for large resource record types causing slow database processing (CVSS 7.5).
- **CVE-2024-0760**: Malicious TCP queries causing server response issues (CVSS 7.5).

Impact of Vulnerabilities:

- **Server Termination**: Exploitation may lead to unexpected termination of server instances.
- **Resource Depletion**: Significant depletion of available CPU resources.
- **Query Processing**: Slowed down query processing by up to 100 times, leading to unresponsiveness.

Patch Releases:

- Patches issued in BIND 9 versions 9.18.28, 9.20.0, and 9.18.28-S1 to address these vulnerabilities.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the patched versions at the earliest.

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://www.openwall.com/lists/oss-security/2024/07/23/1