مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in F5 BIG-IP DNS

Tracking #:432318064

Date:25-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in certain BIND implementations used by BIG-IP DNS resolvers. The issue could allow an attacker to manipulate DNS responses under specific conditions, potentially affecting the integrity of DNS resolution.

TECHNICAL DETAILS:

A vulnerability has been identified in BIND affecting certain versions of BIG-IP DNS resolvers. Due to a weakness in the Pseudo Random Number Generator (PRNG), an attacker could predict the source port and query ID used by BIND, potentially allowing DNS cache poisoning attacks. Successful exploitation may redirect client traffic to attacker-controlled IP addresses.

Vulnerability Details

- CVE-2025-40780
- **Severity: High – CVSS 7.5 (v3.1)**
- A weakness in BIND's PRNG allows attackers to predict DNS query parameters. When exploited, an attacker can inject spoofed DNS records into the resolver cache of a BIG-IP DNS system. Once poisoned, the resolver may return fraudulent DNS responses, allowing attackers to:
    - Redirect users to malicious infrastructure
    - Interfere with service routing
    - Enable further phishing or malware delivery
    - Manipulate traffic flows for data interception

Impact

Exploitation allows attackers to inject malicious or spoofed DNS records into the resolver, resulting in incorrect DNS responses to clients.

Affected Products

- **BIND 9**: Versions 9.16.0–9.16.50, 9.18.0–9.18.39, 9.20.0–9.20.13, 9.21.0–9.21.12, 9.16.8-S1–9.16.50-S1, 9.18.11-S1–9.18.39-S1, 9.20.9-S1–9.20.13-S1
- **BIG-IP DNS**: Versions 15.x, 16.x, 17.x, 21.x

RECOMMENDATIONS:

- Apply all vendor-provided patches addressing this vulnerability as soon as they become available.
- Ensure all affected software is updated to the latest available versions.
- Review DNS configurations and security settings to reduce exposure.
- Monitor DNS activity for unusual or suspicious responses.

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://my.f5.com/manage/s/article/K000157948