Vulnerabilities affecting multiple versions of the BIND 9

September 26, 2022 — v1.0

TLP:WHITE

Summary

On September 21, 2022, the Internet Systems Consortium (ISC) has released security advisories that address vulnerabilities affecting multiple versions of the ISC’s Berkeley Internet Name Domain (BIND) 9. A remote attacker could exploit these vulnerabilities to potentially cause denial-of-service conditions.[1]

Technical Details

From the BIND 9 Security Vulnerability Matrix published by ISC, four vulnerabilities have a 7.5 CVSS Score:

• **CVE-2022-2906** - Memory leaks in code handling Diffie-Hellman key exchange via TKEY RRs (OpenSSL 3.0.0+ only). [2]

Changes between OpenSSL 1.x and OpenSSL 3.0 expose a flaw in named that causes a small memory leak in key processing when using TKEY records in Diffie-Hellman mode with OpenSSL 3.0.0 and later versions. An attacker can leverage this flaw to gradually erode available memory to the point where named crashes for lack of resources. Upon restart the attacker would have to begin again, but nevertheless there is the potential to deny service.

• **CVE-2022-3080** - BIND 9 resolvers configured to answer from stale cache with zero stale-answer-client-timeout may terminate unexpectedly. [3]

BIND 9 resolver can crash when stale cache and stale answers are enabled, option stale-answer-client-timeout is set to 0 and there is a stale CNAME in the cache for an incoming query. By sending specific queries to the resolver, an attacker can cause named to crash.

• **CVE-2022-38177** and **CVE-2022-38178** - Memory leak in ECDSA DNSSEC verification code. [4][5]

The DNSSEC verification code for the ECDSA algorithm leaks memory when there is a signature length mismatch. By spoofing the target resolver with responses that have a malformed ECDSA
signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.

Affected Products

Multiple versions of BIND 9.

Recommendations


References