Security Advisory 2023-041

Multiple Vulnerabilities in BIND 9 DNS System

June 26, 2023 — v1.0

TLP:CLEAR

History:

- *26/06/2023 — v1.0 – Initial publication*

Summary

On June 22, The Internet Systems Consortium (ISC) has released security advisories that address high severity 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

`CVE-2023-2828` (CVSSv3 base score of 7.5)

Every *named* instance configured to run as a recursive resolver maintains a cache database holding the responses to the queries it has recently sent to authoritative servers. The size limit for that cache database can be configured using the *max-cache-size* statement in the configuration file; it defaults to 90% of the total amount of memory available on the host. When the size of the cache reaches 7/8 of the configured limit, a cache-cleaning algorithm starts to remove expired and/or least-recently used RRsets from the cache, to keep memory use below the configured limit.

It has been discovered that the effectiveness of the cache-cleaning algorithm used in *named* can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured *max-cache-size* limit to be significantly exceeded. By exploiting this flaw, an attacker can cause the amount of memory used by a *named* resolver to go well beyond the configured *max-cache-size* limit [2].

`CVE-2023-2829` (CVSSv3 base score of 7.5)

A *named* instance configured to run as a DNSSEC-validating recursive resolver with the Aggressive Use of DNSSEC-Validated Cache (RFC 8198) option (*synth-from-dnssec*) enabled can be remotely terminated using a zone with a malformed NSEC record. By sending specific queries to the resolver, an attacker can cause named to terminate unexpectedly [3].

`CVE-2023-2911` (CVSSv3 base score of 7.5)

If the *recursive-clients* quota is reached on a BIND 9 resolver configured with both *stale-answer-enable yes;* and *stale-answer-client-timeout 0;*, a sequence of serve-stale-related lookups could cause *named* to loop and terminate unexpectedly due to a stack overflow. By sending specific queries to the resolver, an attacker can cause *named* to terminate unexpectedly [4].

ISC is not aware of any active exploits related to the aforementioned vulnerabilities [2,3,4].

Affected Products

`CVE-2023-2828`

BIND [2]:

- 9.11.0 -> 9.16.41
- 9.18.0 -> 9.18.15
- 9.19.0 -> 9.19.13

BIND Supported Preview Edition (a special feature preview branch of BIND provided to eligible ISC support customers) [2]:

- 9.11.3-S1 -> 9.16.41-S1
- 9.18.11-S1 -> 9.18.15-S1

Versions prior to 9.11.37 & 9.11.37-S1 were not assessed, but we believe that all versions of BIND 9.11 are vulnerable. Some even older major branches may be vulnerable as well [2].

`CVE-2023-2829`

BIND Supported Preview Edition [3]:

- 9.16.8-S1 -> 9.16.41-S1
- 9.18.11-S1 -> 9.18.15-S1

`CVE-2023-2911`

BIND [4]:

- 9.16.33 -> 9.16.41
- 9.18.7 -> 9.18.15

BIND Supported Preview Edition [4]:

- 9.16.33-S1 -> 9.16.41-S1
- 9.18.11-S1 -> 9.18.15-S1

BIND 9.11-S versions that support the stale-answer-client-timeout option are not vulnerable[4].

Recommendations

CERT-EU highly recommends update the system to most closely related to your current version of BIND 9:

BIND [2,3,4]:

- 9.16.42
- 9.18.16
- 9.19.14

BIND Supported Preview Edition [2,3,4]:

- 9.16.42-S1
- 9.18.16-S1

Workarounds

- `CVE-2023-2828` - No workarounds known [2].
- `CVE-2023-2829` - Setting *synth-from-dnssec* to *no* prevents the problem [3].
- `CVE-2023-2911` - Setting *stale-answer-client-timeout* to *off* or to a non-zero value prevents the issue. Users of versions 9.18.10, 9.16.36, 9.16.36-S1 or older who are unable to upgrade should set *stale-answer-client-timeout* to *off*; using a non-zero value with these older versions leaves *named* vulnerable to CVE-2022-3924. Although it is possible to set the *recursive-clients* limit to a high number to reduce the likelihood of this scenario, this is not recommended; the limit on *recursive-clients* is important for preventing exhaustion of server resources. The limit cannot be disabled entirely [4].

References

[1] https://www.cisa.gov/news-events/alerts/2023/06/22/isc-releases-security-advisories-multiple-versions-bind-9

[2] https://kb.isc.org/v1/docs/cve-2023-2828

[3] https://kb.isc.org/v1/docs/cve-2023-2829

[4] https://kb.isc.org/v1/docs/cve-2023-2911