BIND Updates Patch High-Severity, Remotely Exploitable DoS Flaws

The Internet Systems Consortium (ISC) this week announced patches for multiple high-severity denial-of-service (DoS) vulnerabilities in the DNS software suite BIND.

The addressed issues could be exploited remotely to cause *named* – the BIND daemon that acts both as an authoritative name server and as a recursive resolver – to crash, or could lead to the exhaustion of the available memory.

The first of the security defects, tracked as CVE-2022-3094, can be exploited by sending a flood of dynamic DNS updates, which would cause *named* to allocate large amounts of memory, resulting in a crash due to a lack of free memory.

According to ISC, because allocated memory is only retained for clients for which access credentials are accepted, the scope of the vulnerability is limited to trusted clients that are allowed to make dynamic zone changes.

For BIND 9.11 and earlier branches, the flaw can be exploited to exhaust internal resources, which results in performance issues, but not a crash.

Tracked as CVE-2022-3736, the second issue leads to a crash "when stale cache and stale answers are enabled, option stale-answer-client-timeout is set to a positive integer, and the resolver receives an RRSIG query," ISC explains. A remote attacker can trigger the bug by sending crafted queries to the resolver.

The third vulnerability, CVE-2022-3924, impacts the implementation of the *stale-answer-client-timeout* option, when

the resolver receives too many queries that require recursion. If the number of clients waiting for recursion to complete is high enough, a race may occur between providing a stale answer to the longest waiting client and sending an early timeout SERVFAIL, causing *named* to crash.

All three vulnerabilities were resolved with the release of BIND versions 9.16.37, 9.18.11, and 9.19.9. ISC says it is not aware of any of these vulnerabilities being exploited, but encourages all users to update their BIND installations as soon as possible.

ISC also warns of CVE-2022-3488, a bug impacting all supported BIND preview edition versions (a special feature preview branch provided to eligible customers).

The issue can be triggered by sending two responses in quick succession from the same nameserver, both ECS pseudo-options, but with the first response broken, causing the resolver to reject the query response. When processing the second response, *named* crashes.

BIND preview edition version 9.16.37-S1 resolves all four security defects. Additional information on the addressed vulnerabilities can be found in the BIND 9 security vulnerability matrix.

Related: BIND Updates Patch High-Severity Vulnerabilities

Related: High-Severity Vulnerabilities Patched in BIND Server

Related: High-Severity DoS Vulnerability Patched in BIND DNS Software

BIND Updates Patch High-Severity, Remotely Exploitable DoS Flaws