February 16, 2024

Overall rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a denial-of-service vulnerability. The processing of responses coming from specially crafted DNSSEC-signed zones can cause CPU exhaustion on a DNSSEC-validating resolver. The vulnerability affects versions prior to BIND 9.16.48, 9.18.24, and 9.19.21.

Technical Details

The attacker crafts a DNS zone with many DNSKEY and RRSIG records, and a standard compliant DNSSEC validator tries all possible combinations of DNSKEY and RRSIG records in the hope of finding the one combination which matches and validates. If the validator does not implement an explicit limit on the amount of work it will do, it can spend an outrageous amount of resources doing useless work. This attack is also asymmetric - the attacker expends relatively little effort to cause the resolver to expend a lot of effort.

This attack is extremely effective against older versions of BIND because DNSSEC validation was historically done in the same processing thread as basically everything else. This design flaw in BIND, together with the unlimited efforts at validation, allowed an attacker to block query processing in BIND for a long time – on the order of minutes or possibly hours on a slow CPU.

By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-50387, CVE-2023-50868
- CVE-2023-50387: KeyTrap - Extreme CPU consumption in DNSSEC validator
- CVE-2023-50868: Preparing an NSEC3 closest encloser proof can exhaust CPU resources
- BIND 9 Security Release and Multi-Vendor Vulnerability Handling, CVE-2023-50387 and CVE-2023-50868
- BIND 9 Security Vulnerability Matrix
- VRM Vulnerability Reports