مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in BIND DNS Software

Tracking #:432316812

Date:31-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The Internet Systems Consortium (ISC) has disclosed two critical vulnerabilities in its widely used Domain Name System (DNS) software, BIND, tracked as CVE-2024-11187 and CVE-2024-12705.

TECHNICAL DETAILS:

The Internet Systems Consortium (ISC) has disclosed two critical vulnerabilities in its widely used Domain Name System (DNS) software, BIND, tracked as CVE-2024-11187 and CVE-2024-12705. These vulnerabilities pose a serious risk of denial-of-service (DoS) attacks on both authoritative DNS servers and resolvers. Exploiting these flaws can lead to resource exhaustion, potentially disrupting the availability of DNS services, and preventing legitimate traffic from reaching targeted systems.

1. **CVE-2024-11187: Resource Exhaustion via Malicious Zones**
   - This vulnerability allows attackers to craft malicious DNS zones that, when queried, generate responses containing an excessive number of records in the "Additional" section. When these responses are queried repeatedly, the targeted server can experience significant CPU consumption, leading to resource exhaustion and service disruption. A vulnerable server may be overwhelmed to the point where it fails to respond to legitimate DNS queries, effectively causing a denial of service.
   - Impact:
     - High CPU usage
     - Service disruption for authoritative DNS servers
     - Potential widespread service outage if exploited in a large-scale attack
   - Mitigation:
     - ISC recommends upgrading to the latest patched BIND versions. As a temporary workaround, administrators can enable the minimal-responses option in the BIND configuration, which reduces the number of records returned in the "Additional" section of DNS responses.

2. **CVE-2024-12705: DNS-over-HTTPS DoS Vulnerability**
   - This vulnerability specifically affects BIND's DNS-over-HTTPS (DoH) implementation. Attackers can exploit this flaw by flooding a DoH resolver with specially crafted HTTP/2 traffic, leading to excessive CPU and memory usage. This can prevent legitimate clients from establishing DoH connections, effectively disrupting the service.
   - Impact:
     - Overwhelming server resources
     - Inability for legitimate clients to connect via DNS-over-HTTPS
     - Denial-of-service attacks against DoH resolvers
   - Mitigation:
     - To mitigate CVE-2024-12705, administrators are advised to disable DNS-over-HTTPS until the patch can be applied. ISC's updated BIND versions include fixes for this vulnerability.

Fixed Versions:

- 9.18.33
- 9.20.5
- 9.21.4

RECOMMENDATIONS:

- ISC has released patched versions of BIND that address both vulnerabilities. It is strongly recommended that organizations upgrade their BIND installations as soon as possible to mitigate the risks associated with these vulnerabilities
- Organizations should monitor DNS traffic for any signs of exploitation of these vulnerabilities. Look for signs of unusual or excessive traffic directed at DNS servers or DoH resolvers that could indicate an ongoing attack.
- Regularly scan systems for known vulnerabilities, including those in BIND and other critical infrastructure software

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://kb.isc.org/docs/cve-2024-12705
- https://kb.isc.org/docs/cve-2024-11187