CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-027

DNS Protocol Vulnerability

May 20, 2020 — v1.0

TLP:WHITE

History:

- *20/05/2020 — v1.0 – Initial publication*

Summary

On 19th of May 2020 a new DNS protocol vulnerability was made public. It was discovered by researchers from Tel Aviv University and the Interdisciplinary Center in Israel [1].

Disclosed vulnerability abuses DNS delegation mechanism to force DNS resolvers to generate more DNS queries to authoritative servers of attacker's choice. Unlike traditional random subdomain attacks, in case of this attack , the queries are generated by resolver itself [2]. The researchers called this attack the **NXNSAttack**. It appears that pretty much all vendors of DNS resolvers are affected [1].

Technical Details

The main principle of NXNSAttack is that attackers are able to amplify a single DNS query toward DNS resolver plus single DNS answer with fake delegations to fire multiple random queries at victim authoritative servers, effectively using standard-compliant DNS resolver as an amplifier for random subdomain attack [2].

The details of the vulnerabilities are as follows.

- Internet Systems Consortium (ISC) BIND does not sufficiently limit the number of fetches performed when processing referrals (CVE-2020-8616) [3]
- NLnet Labs Unbound can be tricked into amplifying an incoming query into a large number of queries directed to a target (CVE-2020-12662) [4]
- Malformed answers from upstream name servers can be used to make Unbound unresponsive (CVE-2020-12663) [4]
- NIC.CZ Knot Resolver before 5.1.1 allows traffic amplification via a crafted DNS answer from an attacker-controlled server (CVE-2020-12667) [5]
- PowerDNS Denial of Service (CVE-2020-10995) [6]

Moreover, PowerDNS Recursor 4.1.16, 4.2.2 and 4.3.1 contain a mitigation to limit the impact of this DNS protocol issue [6].

Finally, DoH (DNS over HTTP) is irrelevant to this vulnerability because it deals with the communication channel between a client and its recursive resolver while the issues are on the communications between the recursive resolver and the authoritative structure [1].

Affected Products

List of all affected products and versions:

- Internet Systems Consortium (ISC) BIND from 9.0.0 up to 9.11.18, from 9.12.0 up to 9.12.4-P2, from 9.14.0 up to 9.14.11, from 9.16.0 up to 9.16.2, and releases from 9.17.0 up to 9.17.1 of the 9.17 experimental development branch. All releases in the obsolete 9.13 and 9.15 development branches. All releases of BIND Supported Preview Edition from 9.9.3-S1 up to 9.11.18-S1 [3];
- All versions of NLnet Labs Unbound up to and including 1.10.0 [4];
- NIC.CZ Knot Resolver before 5.1.1 [5];
- PowerDNS Recursor from 4.1.0 up to and including 4.3.0 is affected [6].

Others products implementing the vulnerable DNS protocol may also be affected.

Recommendations

The security updates were released and CERT-EU highly recommends to upgrade all mentioned DNS software to a non-affected latest version.

References

[1] http://www.nxnsattack.com/

[2] https://en.blog.nic.cz/2020/05/19/nxnsattack-upgrade-resolvers-to-stop-new-kind-of-random-subdomain-attack/

[3] https://kb.isc.org/docs/cve-2020-8616

[4] https://nlnetlabs.nl/downloads/unbound/CVE-2020-12662_2020-12663.txt

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12667

[6] https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2020-01.html