NXNSAttack

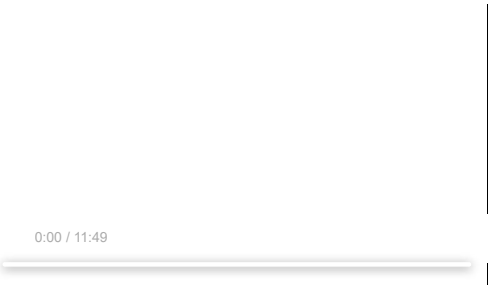
The NXNSAttack is a new vulnerability that exploits the way DNS recursive resolvers operate when receiving NS referral response that contains nameservers but without their corresponding IP addresses (i.e., missing glue-records). The number of DNS messages exchanged in a typical resolution process might be much higher in practice than what is expected in theory, mainly due to a proactive resolution of name-servers' IP addresses. This inefficiency becomes a bottleneck and might be used to mount a devastating attack against either or both, recursive resolvers and authoritative servers. The NXNSAttack is more effective than the NXDomain attack: i) It reaches an amplification factor of more than 1620x on the number of packets exchanged by the recursive resolver. ii) Besides the negative cache, the attack also saturates the 'NS' resolver caches.

A responsible coordinated disclosure procedure has been performed following the discovery of the NXNSAttack described in the paper below. Several DNS software vendors and service providers have adopted measures to protect against the destructive measures of the NXNSAttack.

This work has been accepted for presentation in USENIX Security, August 2020

NXNSAttack was discovered and reported by:

- Yehuda Afek, Tel Aviv University
- Anat Bremler-Barr, The Interdisciplinary Center, Herzliya
- Lior Shafir, Tel Aviv University



NXNSAttack Paper

NXNSAttack Slides

Who was affected? Where can I find official infos/security advisories of involved/affected companies?

	Link
ISC BIND	Security Advisory / CVE-2020-8616
NLnet Labs Unbound	CVE-2020-12662
NIC.CZ Knot Resolver	Blog Post / CVE-2020-12667
PowerDNS	CVE-2020-10995
Google	has been patched
Microsoft	Security Advisory
Cloudflare	has been patched
Amazon	has been patched
Oracle (DYN)	has been patched
Verisign	has been patched
Quad9	has been patched
ICANN	has been patched

Acknowledgements

We would like to thank the anonymous referees for very helpful comments and feedback, and Michael McNally, and Cathy Almond of ISC, Ralph Dolmans, Wouter Wijngaards and Benno Overeinder of NLnet Labs, and Petr Špaček of NIC.CZ, Francis Perron of Google, Remi Gacogne and Peter van Dijk of PowerDNS, John Todd of Quad9, Tim April and Ralf Weber of Akamai and James Adair and Matthew Pozun of Verisign for their help and cooperation in the disclosure procedure, as well as Eyal Ronen and Yair Kaldor for their help in this project.