Date: Sat, 13 Aug 2022 16:59:37 -0700
From: "Philipp Jeitner (SIT)" <philipp.jeitner@....fraunhofer.de>
To: <oss-security@...ts.openwall.com>
Subject: Fixed DNS UDP port in totd DNS forwarder (CVE-2022-34294)

We hereby disclose the discovery of a DNS Cache poisoning vulnerability in totd DNS forwarder. totd is a non-caching DNS forwarder/proxy which has not been further developed for a long time, yet it is still used in some residential router firmwares. Because the projects age, there are no patches available for the described issues.

Our findings are published in our 2022 paper "XDRI Attacks - and - How to Enhance Resilience of Residential Routers" in August 2022.

Discovery/Credits

Philipp Jeitner, Lucas Teichmann and Haya Shulman
Fraunhofer SIT

References

- totd: https://github.com/fwdillema/totd
- paper website: https://xdi-attack.net/
- paper presentation: https://www.usenix.org/conference/usenixsecurity22/presentation/jeitner

CVE-2022-34294: Fixed UDP port in DNS queries sent to upstream resolvers
----

totd uses a fixed UDP source port in upstream queries sent to DNS resolvers which allows DNS cache poisoning as there is not enough entropy to prevent traffic injection attacks.

Summary

The router/forwarder uses a fixed UDP port for all queries sent to upstream resolvers.

Impact

Attackers who control a script or web-site which is loaded on a client of the vulnerable router/forwarder can exploit this to poison the DNS cache by classic DNS poisoning attacks with spoofed IP address of the upstream resolver.

Steps to reproduce

Connect a computer to the vulnerable router/forwarder and trigger multiple DNS queries. Observe the queries sent to upstream resolvers via packet capture, either on the routers Internet-facing interface or the upstream resolver's network interface. The queries captured on these interfaces have the same UDP source port (port 1024 in our tests).

Detailed description and publication timeline

This attack is known to be practical since the 2008 publication "Black Ops 2008: It’s The End Of The Cache As We Know It" (https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf).
During an evaluation of DNS vulnerabilities in routers, we found this attack to be still applicable.

Powered by blists - more mailing lists