Date: Sat, 13 Aug 2022 17:00:16 -0700
From: "Philipp Jeitner (SIT)" <philipp.jeitner@....fraunhofer.de>
To: <oss-security@...ts.openwall.com>
Subject: Multiple DNS Cache poisoning vulnerabilities in dproxy and
 drpoxy-nexgen (CVE-2022-33988, CVE-2022-33989, CVE-2022-33990,
 CVE-2022-33991)

We hereby disclose the discovery of multiple DNS Cache poisoning
vulnerabilities in the dproxy(-nexgen) DNS forwarder. dproxy is a
caching DNS forwarder/proxy which is unmaintained since about 2004, yet
it is still used in some residential router firmwares. Because the
project is unmaintained, 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

   - dproxy: https://sourceforge.net/projects/dproxy/
   - paper website: https://xdi-attack.net/
   - paper presentation:
https://www.usenix.org/conference/usenixsecurity22/presentation/jeitner

CVE-2022-33990: Misinterpretation of special characters in domain names
leading to cache-poisoning

Misinterpretation of special domain name characters in dproxy-nexgen
leads to cache-poisoning as domain names and their associated IP
addresses are cached in their misinterpreted form.

Summary

Attacker can poison the DNS cache of the vulnerable router/forwarder by
triggering queries to attacker controlled domain names whose queries
and/or answers contain special characters (zero-byte or period sign).
These characters are misinterpreted by the vulnerable router/forwarder
so that the attacker can provide addresses for domain names he does not own.

Impact

Attackers who control a script or web-site which is loaded on a client
of the vulnerable router/forwarder can hijack connections by poisoning
the DNS cache.

Steps to reproduce

To reproduce, connect a computer to the router and follow the Steps at
https://xdi-attack.net/manual.html or use our downloadable test-tool at
https://xdi-attack.net/test.html (NOT the online test).

Detailed description and publication timeline

A detailed description of this attack is included in our 2021 USENIX
security paper "Injection Attacks Reloaded: Tunnelling Malicious

Payloads over DNS", see Section 3.2. We conducted further research and found that these attacks apply to various router models.

CVE-2022-33989: Static UDP port in DNS queries sent to upstream resolvers
---

dproxy-nexgen uses a static UDP source port (selected randomly only at boot-time) 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.

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.

CVE-2022-33988: DNS TXID value is re-used from client queries
---

dproxy-nexgen re-uses the DNS transaction id (TXID) value from client queries, which allows attackers able to sent queries to the resolver to conduct DNS cache poisoning attacks as the TXID value is known to the attacker.

Summary

The router/forwarder re-uses the DNS TXID value from client queries when forwarding the DNS query to upstream resolvers.

Impact

Attackers which can send DNS queries directly to the vulnerable router/forwarder can infer the TXID used for upstream queries as the value is re-used from the query sent by the attacker. This allows the attacker to inject malicious records into the router/forwarder's DNS cache, as the remaining entropy in the DNS request (max 16-bit UDP source port) is not enough to protect against spoofed DNS responses.

Steps to reproduce

Connect a computer to the vulnerable router/forwarder and trigger some DNS queries. Monitor the requests sent by the client device (e.g. via wireshark) and compare the DNS TXID value with the value of the packets forwarded to the upstream resolvers, e.g. by capturing traffic on the routers Internet-facing interface or the upstream resolver's network interface. The TXID values of these packets are the same.

```
CVE-2022-33991: Disabling of DNSSEC protection provided by upstream
resolvers
-------------------------------------------------------------------------------

dproxy-nexgen forwards and caches DNS queries with checking disabled
(CD) bit set to 1 which leads to disabling of DNSSEC protection provided
by upstream resolvers.

## Summary

The router/forwarder forwards DNS queries with the checking disabled
(CD) bit set to 1 to upstream resolvers and caches the responses
provided by the upstream resolver. The cached answers are then sent to
other clients even when they do set the checking disabled (CD) bit to 0.

## Impact

Attackers which can send DNS queries directly to the vulnerable
router/forwarder can disable DNSSEC protection on the upstream resolver
by sending queries with the checking disabled (CD) bit set to 1. When
the attacker is able to inject DNS responses via another method (e.g.
MitM attacks, BGP hijacking), this allows attacker to hijack connections
from clients of the vulnerable router/forwarder, as DNSSEC protection is
not guaranteed anymore.

## Steps to reproduce

Connect a computer to the vulnerable router/forwarder and trigger the
following DNS queries via `dig`:

      $ dig sigfail.verteiltesysteme.net +cdflag @router/forwarder-ip
      (should always return 134.91.78.139)

      $ dig sigfail.verteiltesysteme.net +short @router/forwarder-ip
      (returns 134.91.78.139 if vulnerable, should return nothing)

Note: you can replace `sigfail.verteiltesysteme.net` with any other
domain with broken DNSSEC, such as `www.dnssec-failed.org`, only the
addresses will be different.
```