Alpine Linux - Bug #9720

[3.8] pdns-recursor: Multiple vulnerabilities (CVE-2018-10851, CVE-2018-14626, CVE-2018-14644, CVE-2018-16855)

11/29/2018 11:54 AM - Alicha CH

Status:	Closed	**Start date:**	11/29/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-10851, CVE-2018-14626, CVE-2018-14644, CVE-2018-16855

Description

CVE-2018-10851: Crafted answer can cause a denial of service¶

An issue has been found in PowerDNS Recursor allowing a malicious authoritative server to cause a memory leak by sending specially crafted records.
The issue is due to the fact that some memory is allocated before the parsing and is not always properly released if the record is malformed.

Affects: PowerDNS Recursor from 3.2 up to and including 4.1.4

Not affected: 4.1.5, 4.0.9

References:

https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2018-04.html
https://www.openwall.com/lists/oss-security/2018/11/06/8

CVE-2018-14626: Packet cache pollution via crafted query

An issue has been found in PowerDNS Recursor allowing a remote user to craft a DNS query that will cause an answer without DNSSEC records to be inserted into the packet cache and be returned to clients asking for DNSSEC records, thus hiding the presence of DNSSEC signatures for a specific qname and qtype. For a DNSSEC-signed domain, this means that clients performing DNSSEC validation by themselves might consider the answer to be bogus until it expires from the packet cache, leading to a denial of service.

Affects: PowerDNS Recursor from 4.0.0 up to and including 4.1.4

Not affected: 4.1.5, 4.0.9

References:

https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2018-06.html
https://www.openwall.com/lists/oss-security/2018/11/06/8

CVE-2018-14644: Crafted query for meta-types can cause a denial of service¶

An issue has been found in PowerDNS Recursor where a remote attacker sending a DNS query for a meta-type like OPT can lead to a zone being wrongly cached as failing DNSSEC validation. It only arises if the parent zone is signed, and all the authoritative servers for that parent zone answer with FORMERR to a query for at least one of the meta-types. As a result, subsequent queries from clients requesting DNSSEC validation will be answered with a ServFail.

Affects: PowerDNS Recursor from 4.0.0 up to and including 4.1.4

Not affected: 4.0.9, 4.1.5

References:

https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2018-07.html
https://www.openwall.com/lists/oss-security/2018/11/06/8

CVE-2018-16855: Crafted query can cause a denial of service

An issue has been found in PowerDNS Recursor where a remote attacker sending a DNS query can trigger an out-of-bounds memory read while computing the hash of the query for a packet cache lookup, possibly leading to a crash.

Affects: PowerDNS Recursor from 4.1.0 up to and including 4.1.7

Not affected: 4.0.x, 4.1.8

References:

https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2018-09.html

Associated revisions

Revision 25d9fe89 - 12/18/2018 04:14 PM - Natanael Copa

community/pdns-recursor: security upgrade to 4.1.8

fixes #9720

History

#1 - 12/04/2018 10:11 AM - Alicha CH

- Description updated

#2 - 12/18/2018 04:15 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:25d9fe89a4cbd43e9f7cc3e4f9c28cf372f28c57.

#3 - 12/20/2018 01:52 PM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed