Alpine Linux - Bug #9719

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

11/29/2018 11:50 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

Description

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

An issue has been found in PowerDNS Authoritative Server allowing an authorized user to cause a memory leak by inserting a specially crafted record in a zone under their control,
then sending a DNS query for that record. 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 Authoritative from 3.3.0 up to and including 4.1.4

Not affected: 4.1.5, 4.0.6

References:

https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2018-03.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 Authoritative Server 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 DNSSEC validating clients will consider the answer to be bogus until it expires from the packet cache, leading to a denial of service.

Affects: PowerDNS Authoritative from 4.1.0 up to and including 4.1.4

Not affected: 4.1.5, 4.0.x

References:

https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2018-05.html
https://www.openwall.com/lists/oss-security/2018/11/06/8

Associated revisions

Revision 43dd52bd - 11/29/2018 04:08 PM - Natanael Copa

community/pdns: security upgrade to 4.0.6 (CVE-2018-10851)

fixes #9719

History

#1 - 11/29/2018 04:09 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:43dd52bda87e3f1fd92433e5e9a42273dcdfec51.

#2 - 12/04/2018 10:12 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed