Alpine Linux - Bug #6676

Bug # 6674 (Closed): bind: Multiple security issues (CVE-2016-9131, CVE-2016-9147, CVE-2016-9444)

[3.5] bind: Multiple security issues (CVE-2016-9131, CVE-2016-9147, CVE-2016-9444)

01/12/2017 03:28 PM - Alicha CH

Status:	Closed	**Start date:**	01/12/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.1		
Affected versions:		**Security IDs:**	

Description

CVE-2016-9131: A malformed response to an ANY query can cause an assertion failure during recursion

A malformed query response received by a recursive server in response to a query of RTYPE ANY could trigger an assertion failure while named is attempting to add the RRs in the query response to the cache. While the combination of properties which triggers the assertion should not occur in normal traffic, it is potentially possible for the assertion to be triggered deliberately by an attacker sending a specially-constructed answer having the required properties, after having engineered a scenario whereby an ANY query is sent to the recursive server for the target QNAME. A recursive server will itself only send a query of type ANY if it receives a client query of type ANY for a QNAME for which it has no RRsets at all in cache, otherwise it will respond to the client with the the RRsets that it has available.

Affected versions:

9.4.0 -> 9.6-ESV-R11-W1, 9.8.5 -> 9.8.8, 9.9.3 -> 9.9.9-P4, 9.9.9-S1 -> 9.9.9-S6, 9.10.0 -> **9.10.4-P4**, 9.11.0 -> 9.11.0-P1

Fixed in:

BIND 9 version 9.9.9-P5
BIND 9 version 9.10.4-P5
BIND 9 version 9.11.0-P2

Reference:

https://kb.isc.org/article/AA-01439/0

CVE-2016-9147: An error handling a query response containing inconsistent DNSSEC information could cause an assertion failure

Depending on the type of query and the EDNS options in the query they receive, DNSSEC-enabled authoritative servers are expected to include RRSIG and other RRsets in their responses to recursive servers. DNSSEC-validating servers will also make specific queries for DS and other RRsets. Whether DNSSEC-validating or not, an error in processing malformed query responses that contain DNSSEC-related RRsets that are inconsistent with other RRsets in the same query response can trigger an assertion failure. Although the combination of properties which triggers the assertion should not occur in normal traffic, it is potentially possible for the assertion to be triggered deliberately by an attacker sending a specially-constructed answer.

Affected versions:

9.9.9-P4, 9.9.9-S6, **9.10.4-P4**, 9.11.0-P1

Fixed in:

BIND 9 version 9.9.9-P5
BIND 9 version 9.10.4-P5
BIND 9 version 9.11.0-P2

Reference:

https://kb.isc.org/article/AA-01440/0

CVE-2016-9444: An unusually-formed DS record response could cause an assertion failure

An unusually-formed answer containing a DS resource record could trigger an assertion failure. While the combination of properties which triggers the assertion
should not occur in normal traffic, it is potentially possible for the assertion to be triggered deliberately by an attacker sending a specially-constructed answer having the required properties.

Affected versions:

9.6-ESV-R9 -> 9.6-ESV-R11-W1, 9.8.5 -> 9.8.8, 9.9.3 -> **9.9.9-P4**, 9.9.9-S1 -> 9.9.9-S6, 9.10.0 -> 9.10.4-P4, 9.11.0 -> 9.11.0-P1

Fixed in:

BIND 9 version 9.9.9-P5
BIND 9 version 9.10.4-P5
BIND 9 version 9.11.0-P2

Reference:

https://kb.isc.org/article/AA-01441/0

Associated revisions

Revision db19c120 - 01/13/2017 09:21 AM - Sergei Lukin

main/bind: security upgrade to 9.10.4_p5 - fixes #6676

CVE-2016-9131: A malformed response to an ANY query can cause an assertion failure during recursion
CVE-2016-9147: An error handling a query response containing inconsistent DNSSEC information could cause an assertion failure
CVE-2016-9444: An unusually-formed DS record response could cause an assertion failure

History

#1 - 01/13/2017 09:26 AM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:db19c120bc6d032b9f6fa773b7875be828dcfd62.

#2 - 01/16/2017 08:51 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed