Alpine Linux - Bug #7438

Bug # 7436 (Closed): bind: An error processing RPZ rules can cause named to loop endlessly after handling a query (CVE-2017-3140)

[3.6] bind: An error processing RPZ rules can cause named to loop endlessly after handling a query (CVE-2017-3140)

06/16/2017 08:20 AM - Alicha CH

Status:	Closed	**Start date:**	06/16/2017
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.6.2		
Affected versions:		**Security IDs:**	

Description

If named is configured to use Response Policy Zones (RPZ) an error processing some rule types can lead to
a condition where BIND will endlessly loop while handling a query.

Impact:

A server is potentially vulnerable to degradation of service if

1. the server is configured to use RPZ,
2. the server uses NSDNAME or NSIP policy rules, and
3. an attacker can cause the server to process a specific query

Successful exploitation of this condition will cause named to enter a state where it continues to loop while processing the query without ever reaching an end state.
While in this state, named repeatedly queries the same sets of authoritative nameservers and this behavior will usually persist indefinitely beyond the normal client
query processing timeout. By triggering this condition multiple times, an attacker could cause a deliberate and substantial degradation in service.
Operators of servers that meet the above conditions 1. and 2. may also accidentally encounter this defect during normal operation. It is for this reason that the decision
was made to issue this advisory despite its low CVSS score.

Affected versions:

9.9.10, 9.10.5, **9.11.0**->9.11.1, 9.9.10-S1, 9.10.5-S1

Fixed in:

BIND 9 version **9.11.1-P1**

Reference:

https://kb.isc.org/article/AA-01495/74/CVE-2017-3140%3A-An-error-processing-RPZ-rules-can-cause-named-to-loop-endlessly-after-handling-a-query.html

Associated revisions

Revision dab03646 - 06/16/2017 02:17 PM - Natanael Copa

main/bind: security upgrade to 9.11.1_p1 (CVE-2017-3140)

fixes #7438

History

#1 - 06/16/2017 02:32 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:dab0364651fea7158196224398355ee204826bf0.

#2 - 06/29/2017 07:13 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed