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

Author: **Michael McNally** Reference Number: **AA-01440** Views: **52829** Created: **2017-01-11 10:31** **0 Rating**/ Voters
Last Updated: **2017-01-11 22:36**

CVE:	CVE-2016-9147
Document Version:	2.0
Posting date:	11 Jan 2017
Program Impacted:	BIND
Versions affected:	9.9.9-P4, 9.9.9-S6, 9.10.4-P4, 9.11.0-P1
Severity:	High
Exploitable:	Remotely

Description:

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.

Impact:

This vulnerability occurs during the processing of an answer packet received in response to a query. As a result, recursive servers are at the greatest risk; authoritative servers are at risk only to the extent that they perform a limited set of queries (for example, in order to do zone service - see https://kb.isc.org/article/AA-00914/55/Why-does-my-authoritative-only-nameserver-try-to-query-the-root-nameservers.html). There are several variations of malformed query response that can cause an assertion failure, some of which will trigger a failure on recursive servers that are not DNSSEC-validating.

Successful exploitation of this vulnerability will cause named to encounter an assertion failure and stop executing, resulting in denial of service to clients.

CVSS Score: 7.5

CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

For more information on the Common Vulnerability Scoring System and to obtain your specific environmental score please visit:
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Workarounds:

None known.

Active exploits:

No known active exploits.

Solution: Upgrade to the patched release most closely related to your current version of BIND. These can all be downloaded from http://www.isc.org/downloads.

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

BIND Supported Preview Edition is a special feature preview branch of BIND provided to eligible ISC support customers.

- BIND 9 version 9.9.9-S7

Document Revision History:

1.0 Advance Notification, 03 January 2017
1.1 Updated Versions affected to include 9.9.9-S6 and Solution to include 9.9.9-S7, 09 January 2017
2.0 Public Announcement, 11 January 2017

Related Documents:

See our BIND9 Security Vulnerability Matrix at https://kb.isc.org/article/AA-00913 for a complete listing of Security Vulnerabilities and versions affected.
If you'd like more information on ISC Subscription Support and Advance Security Notifications, please visit http://www.isc.org/support/.

Do you still have questions? Questions regarding this advisory should go to security-officer@isc.org. *To report a new issue, please encrypt your message using security-officer@isc.org's PGP key which can be found here: https://www.isc.org/downloads/software-support-policy/openpgp-key/. If you are unable to use encrypted email, you may also report new issues at: https://www.isc.org/community/report-bug/.*

Note: ISC patches only currently supported versions. When possible we indicate EOL versions affected. (For current information on which versions are actively supported, please see http://www.isc.org/downloads/).

ISC Security Vulnerability Disclosure Policy: Details of our current security advisory policy and practice can be found here https://kb.isc.org/article/AA-00861/164/ISC-Software-Defect-and-Security-Vulnerability-Disclosure-Policy.html

This Knowledge Base article https://kb.isc.org/article/AA-01440 is the complete and official security advisory document.

For assistance with problems and questions for which you have not been able to find an answer in our Knowledge Base, we recommend searching our community mailing list archives and/or posting your question there (you will need to register there first for your posts to be accepted). The bind-users and the dhcp-users lists particularly have a long-standing and active membership.

ISC relies on the financial support of the community to fund the development of its open source software products. If you would like to support future product evolution and maintenance as well having peace of mind knowing that our team of experts are poised to provide you with individual technical assistance whenever you call upon them, then please consider our Professional Subscription Support services - details can be found on our main website.