CVE-2016-9778: An error handling certain queries using the nxdomain-redirect feature could cause a REQUIRE assertion failure in db.c

Author: **Michael McNally** Reference Number: **AA-01442** Views: **117582** Created: **2017-01-11 10:31** **0 Rating**/ Voters
Last Updated: **2017-01-11 22:35**

CVE: CVE-2016-9778
Document Version: 2.0
Posting date: 11 Jan 2017
Program Impacted: BIND
Versions affected: 9.9.8-S1 -> 9.9.8-S3, 9.9.9-S1 -> 9.9.9-S6, 9.11.0-9.11.0 -> P1
Severity: High (for affected configurations)
Exploitable: Remotely

Description:

An error in handling certain queries can cause an assertion failure when a server is using the nxdomain-redirect feature to cover a zone for which it is also providing authoritative service. A vulnerable server could be intentionally stopped by an attacker if it was using a configuration that met the criteria for the vulnerability and if the attacker could cause it to accept a query that possessed the required attributes.

Please note: This vulnerability affects the "nxdomain-redirect" feature, which is one of two methods of handling NXDOMAIN redirection, and is only available in certain versions of BIND. Redirection using zones of type "redirect" is not affected by this vulnerability.

Impact:

Only servers which are performing NXDOMAIN redirection using the "nxdomain-redirect" function are potentially vulnerable and then only a subset of those servers. In order to be affected a server must be using nxdomain-redirect AND must be redirecting NXDOMAIN responses for a zone for which the server also provides authoritative service -- therefore a purely recursive server is not at risk, either. Successful exploitation of the vulnerability will cause named to stop execution after encountering a REQUIRE assertion failure in db.c, resulting in denial of service to clients.

CVSS Score: 7.5

CVSSv3 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:

Either provide an ordinary (that is: not redirected) NXDOMAIN for non-existent resource records in zones for which authoritative data is served on the same server or use redirect zones instead of the nxdomain-redirect feature.

Active exploits:

No known active exploits.

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

- BIND 9 version 9.11.0-P2

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

- BIND 9.9.9-S7

Document Revision History:

1.0 Advance Notification, 03 January 2017
1.1 Updated Versions affected to include 9.11.0-P1, 04 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 visithttp://www.isc.org/support/.

Do you still have questions? Questions regarding this advisory should go tosecurity-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 herehttps://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-01442 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.