CVE-2016-2776: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request

Author: **Brian Conry** Reference Number: **AA-01419** Views: **120250** Created: **2016-09-27 08:30** **0 Rating**/ Voters
Last Updated: **2016-10-04 20:16**

CVE: CVE-2016-2776
Document Version: 2.1
Posting date: 2016-09-27
Program Impacted: BIND
Versions affected: 9.0.x -> 9.8.x, 9.9.0->9.9.9-P2, 9.9.3-S1->9.9.9-S3, 9.10.0->9.10.4-P2, 9.11.0a1->9.11.0rc1
Severity: High
Exploitable: Remotely

Description:

Testing by ISC has uncovered a critical error condition which can occur when a nameserver is constructing a response. A defect in the rendering of messages into packets can cause named to exit with an assertion failure in buffer.c while constructing a response to a query that meets certain criteria.

This assertion can be triggered even if the apparent source address isn't allowed to make queries (i.e. doesn't match 'allow-query').

Impact:

All servers are vulnerable if they can receive request packets from any source.

CVSS Score: 7.8

CVSS Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:C)

For more information on the Common Vulnerability Scoring System and to obtain your specific environmental score please visit: http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C)

Workarounds:

No practical workarounds exist.

Active exploits:

A step-by-step breakdown of the issue has been published and working Metasploit code is available. Crashes have been reported that appear to be the result active exploitation.

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

- BIND 9 version 9.9.9-P3
- BIND 9 version 9.10.4-P3
- BIND 9 version 9.11.0rc3

BIND 9 Supported Preview edition is a feature preview version ofBIND provided exclusively to eligible ISC Support customers.

- BIND 9 version 9.9.9-S5

Document Revision History:
1.0 2016-09-14 - Advance Notification
1.1 2016-09-21 - Added information about the Stable Preview release to versions affected. Updated solution section to reflect replacing 9.11.0rc2 with 9.11.0rc3 and 9.9.9-S4 with 9.9.9-S5.
2.0 2016-09-27 - Posting date changed and public disclosure.
2.1 2016-10-04 - Updated 'Active exploits' section.

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-01419 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.