1 Release Notes for BIND Version 9.10.3-P4

1.1 Introduction

This document summarizes changes since BIND 9.10.3:

BIND 9.10.3-P4 addresses the security issues described in CVE-2016-1285, CVE-2016-1286 and CVE-2016-2088.

BIND 9.10.3-P3 addresses the security issues described in CVE-2015-8704 and CVE-2015-8705. It also fixes a serious regression in authoritative server selection that was introduced in BIND 9.10.3.

BIND 9.10.3-P2 addresses the security issues described in CVE-2015-3193 (OpenSSL), CVE-2015-8000 and CVE-2015-8461.

BIND 9.10.3-P1 was incomplete and was withdrawn prior to publication.

1.2 Download

The latest versions of BIND 9 software can always be found at <http://www.isc.org/downloads/>. There you will find additional information about each release, source code, and pre-compiled versions for Microsoft Windows operating systems.

1.3 Security Fixes

- Duplicate EDNS COOKIE options in a response could trigger an assertion failure. This flaw is disclosed in CVE-2016-2088. [RT #41809]
- The resolver could abort with an assertion failure due to improper DNAME handling when parsing fetch reply messages. This flaw is disclosed in CVE-2016-1286. [RT #41753]
- Malformed control messages can trigger assertions in named and rndc. This flaw is disclosed in CVE-2016-1285. [RT #41666]
- Certain errors that could be encountered when printing out or logging an OPT record containing a CLIENT-SUBNET option could be mishandled, resulting in an assertion failure. This flaw is disclosed in CVE-2015-8705. [RT #41397]
- Specific APL data could trigger an INSIST. This flaw is disclosed in CVE-2015-8704. [RT #41396]
- Named is potentially vulnerable to the OpenSSL vulnerability described in CVE-2015-3193.
- Incorrect reference counting could result in an INSIST failure if a socket error occurred while performing a lookup. This flaw is disclosed in CVE-2015-8461. [RT#40945]
- Insufficient testing when parsing a message allowed records with an incorrect class to be be accepted, triggering a REQUIRE failure when those records were subsequently cached. This flaw is disclosed in CVE-2015-8000. [RT #40987]

1.4 New Features

- None.

1.5 Feature Changes

- Updated the compiled in addresses for H.ROOT-SERVERS.NET.

1.6 Bug Fixes

- Authoritative servers that were marked as bogus (e.g. blackholed in configuration or with invalid addresses) were being queried anyway. [RT #41321]

1.7 End of Life

The end of life for BIND 9.10 is yet to be determined but will not be before BIND 9.12.0 has been released for 6 months. <https://www.isc.org/downloads/software-support-policy/>

1.8 Thank You

Thank you to everyone who assisted us in making this release possible. If you would like to contribute to ISC to assist us in continuing to make quality open source software, please visit our donations page at <http://www.isc.org/donate/>.