Security Advisory Report - OBSO-1610-02

ISC BIND Nameserver Denial of Service Vulnerabilities (CVE-2016-2776, CVE-2016-2848)

Creation Date: 2016-10-25
Last Update: 2016-10-25

Summary

In September and October 2016, two vulnerabilities were reported by ISC (Internet Systems Consortium) for the DNS nameservice implementation BIND which could allow unauthenticated remote attackers to terminate a DNS server via specially crafted DNS request packets.
The CVE IDs CVE-2016-2776 and CVE-2016-2848 were assigned.
This advisory describes the impact to Unify products and associated recommended actions.

The risk is rated **medium** for

- OpenScape Voice V9 (in OpenScape Enterprise Express V9 installations)
- OpenScape Branch
- OpenScape SBC

Vulnerability Details

The BIND nameservice (named) on OpenScape Voice, OpenScape Branch, and OpenScape SBC may crash when constructing the response after having received specially crafted query packets on port 53/upd or port 53/tcp (CVE-2016-2776).
A similar effect may be caused by a vulnerability that existed, when earlier versions of BIND receive packets with malformed options (CVE-2016-2848). However, this vulnerability affects only older versions of OpenScape Voice, Branch or SBC that are out of software support already (i.e. before V7).

For further details refer to the Security Advisories published by ISC for CVE-2016-2776 and for CVE-2016-2848.

Affected Products

Products confirmed as vulnerable with medium risk:

- OpenScape Branch and SBC: V7 and V8 (all versions) and V9 before V9 R0.11.0
- OpenScape Voice V9 (in OpenScape Enterprise Express V9 installations)

CVSSv3 scores:

- Base Score: 5.3 (Medium)
- Temporal Score 5.1 (Medium) for OpenScape Branch and SBC
  CVSS v3 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:H/RL:O/RC:C)
- Temporal Score: 5.3 (Medium) for OpenScape Enterprise Express V9
  CVSS v3 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:H/RL:U/RC:C)

Products using the BIND nameservice implementation, but confirmed as not vulnerable:

- OpenScape 4000
- OpenStage Diagnostic Data Collector

Products using the BIND nameservice implementation, where investigation is ongoing:

- OpenScape Contact Center Call Director SIP Service (CDSS)

Recommended Actions

- OpenScape Branch and SBC: update to V9 R0.11.0 (release date: 2016-10-14) or any later version. No fix releases are planned for V7 or V8.
- OpenScape Voice V9 in OpenScape Enterprise Express (OSEE) installations: fix release pending.

Additional Mitigation Information:

In default installations, OpenScape Voice, Branch and SBC are not vulnerable, as the DNS Server is disabled.

OpenScape Branch and SBC:
OpenScape Branch and SBC are only affected if the DNS Server is enabled and configured as Slave or Master, but not when configured as Forwarding DNS Server.
In a DNS Slave configuration, restrict the DNS zones to trusted zones only and configure a trusted master DNS server only.

OpenScape Enterprise Express (OSEE) V9:
In OSEE V9 installations, the DNS service is enabled on the OpenScape Voice node to resolve domain names for all systems within the OSEE internal network. External - potentially malicious - DNS packets are transferred transparently from OpenScape SBC (acting as Forwarding Name Server) to OpenScape Voice. In those installations it is therefore more important to update OpenScape Voice, than OpenScape SBC.

References

- ISC Security Advisories: CVE-2016-2776 and CVE-2016-2848
- SUSE Security Advisories: CVE-2016-2776 and CVE-2016-2848

Revision History

2016-10-25: Initial release

Advisory ID: OBSO-1610-02 (a=156), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.
All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.