# Security Advisory Report - OBSO-1602-02

## Glibc libresolv - Stack-based Buffer Overflow Vulnerability (CVE-2015-7547)

Creation Date: 2016-02-19
Last Update: 2016-04-29

## Summary

On Feb 16, 2016 a vulnerability in the libresolv library of the GNU glibc implementation was reported that may allow remote unauthenticated attackers to cause a Denial of Service for various Linux based applications and services, or potentially allow code execution on affected systems.
The vulnerability was discovered concurrently by the Google Security Team and RedHat.
CVE ID CVE-2015-7547 was assigned.

The risk is rated **high** for

- OpenScape 4000 Softgate (in SIP Service Provider scenario)
- OpenScape Branch, OpenScape SBC and Circuit Premise Universal Telephony Connector
- OpenStage Xpert 6010p terminals (Linux)

The risk is rated **medium or low** for some other Unify products.

This advisory describes the impact to Unify products and associated recommended actions.

## Vulnerability Details

The DNS (Domain Name System) client side resolver (libresolv library) as shipped with the glibc package (versions 2.9 to 2.22) on Linux based systems is vulnerable to a stack-based buffer overflow when the getaddrinfo() library function is used. Ths issue is caused by an error in the buffer management when performing dual A/AAAA (IPv4/IPv6 address record) DNS queries.

Any software using this function may be exploited by specially crafted DNS response packets sent by an attacker-controlled DNS name server or through a man-in-the-middle attack. This may lead to code execution on the vulnerable Linux based system in the context of the client application that executed the associated DNS query.

For more information refer to the public disclosure of the issue and the associated blog post by the Google Security Team.

**CVSSv3 scores for Unify products**: see individual scores in the section "Affected Products" below.

## Affected Products

**Products confirmed as vulnerable with high risk:**

- OpenScape 4000 Softgate (only in SIP Provider scenarios)
- OpenScape Branch, OpenScape SBC and Circuit Premise Universal Telephony Connector
- OpenStage Xpert 6010p terminals (Linux)

CVSSv3 scores:

- Base Score: 7.4 (High)
- Temporal Score 6.6 (Medium)
- CVSS v3 Vector (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H/E:U/RL:W/RC:C)

**Products confirmed as vulnerable with medium risk:**

- OpenScape Voice
- OpenScape Business and OpenScape Office (only in installations with UC features enabled)
- OpenScape Contact Center Call Director SIP Service (CDSS)

CVSSv3 scores:

- Base Score: 4.8 (Medium)
- Temporal Score 4.3 (Medium)
- CVSS v3 Vector (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L/E:U/RL:W/RC:C)

**Products confirmed as vulnerable with low risk:**

- OpenScape 4000 Assistant, CSTA, Platform
- OpenScape 4000 Softgate (other scenarios than SIP Provider)

**Products confirmed as not vulnerable:**

- OpenStage / OpenScape Desk Phone IP SIP and HFA
- OpenScape Alarm Response (OScAR) Eco and Pro
- HiPath Cordless IP
- Unify apps running on Apple iOS or Google Android
- Unify products running on Microsoft Windows; including OpenStage Xpert 6010p (Windows)

**Unify Application Server Products:**
No high risk scenario was determined for any application that runs on standard Linux Operating Systems, including OpenScape UC Application (Frontend, Backend, Media Server, Facade Server), OpenScape Common Management Platform, OpenScape Voice Survival Authority, OpenScape 4000 Manager, OpenScape Business S and Booster Server (all running on SUSE SLES 11 SP3 or SP4), and OpenScape Xpert MLC (running on Debian Linux).
However it is recommended to apply the corresponding Operating System updates at the earliest opportunity, as documented in section 3. below.

## Recommended Actions

**1. General recommendations:**

- Ensure that only trusted DNS servers are operated in your / your customer's network.
  If they are impacted by CVE-2015-7547, apply accociated patches or other mitigation measures as provided by the corresponding DNS server's vendor.
- Review the network configuration of affected Unify products to ensure that the DNS server configuration lists only trusted (and patched) DNS servers as determined in the bullet above.
  (Ensure similar for any other systems in your network.)
- At network boundaries (esp. towards the WAN/Internet), apply appropriate firewall rules to block any outgoing DNS requests, unless they are originated from the configured trusted DNS server(s).

**2. Embedded Devices and Software Appliances:**
Apply the corresponding Unify product updates:

- **OpenStage Xpert 6010p (Linux)**: A firmware that fixes CVE-2015-7547 is available (release date: 2016-02-24) and can be installed on any customer site. For details contact your support representative at Unify.
- **OpenScape Branch, OpenScape SBC and Circuit Premise Universal Telephony Connector V8 R1:** Update to V8 R1.7.0 (release date: 2016-03-11) or any later version
- **OpenScape Branch and OpenScape SBC V7 R1**: Update to V7 R1.34.0 (release date: 2016-03-08) or any later version.
  Note: End of support for V7 R1 has already been announced; this release only fixes CVE-2015-7547. Unlike in V8 R1 or V9, less critical security vulnerabilities are no longer addressed in V7 R1. We recommend to upgrade to V8 R1 or V9.
- **OpenScape 4000 V7 R2:** Install Hotfix V7 R2.23.2 (HF004427, release date: 2016-04-11).
- **OpenScape 4000 V7 R1:** Install Hotfix V7 R1.39.6 (HF004402, release date: 2016-03-15).
  Note: In accordance with the Unify Product Lifecycle Policy (PLP) future Hot Fix deliveries will be based on the latest version. We therefore recommend to upgrade to OpenScape 4000 V7 R2.23.2 or any later version.
- **HiPath 4000 V6 R2:** Install Hotfix V6 R2.17.8 (HF004401, release date: 2016-03-15).
  Note: HiPath 4000 V6 R2 has achieved end of support on 2016-02-29; this hotfix only addresses CVE-2015-7547. We recommend to upgrade to OpenScape 4000 V7 R2.23.2 or any later version.
- **OpenScape Contact Center Call Director SIP Service (CDSS):** Update to V9 R0.1.11338 (INF-16-000202, release date: 2016-03-22).
  Note: CDSS V8 is no longer sustained; instead, install the latest release of CDSS V9, which is released for both V8 and V9 Contact Center solutions.
- **OpenScape Voice V8 R1:** Install V8 R1.44.0 Images (V8.00.01.ALL.08_PS0044, INF-16-000123, release date: 2016-03-23).
- **OpenScape Voice V7 R1:** Install V8 R1.51.4 Images (V7.00.01.ALL.07_PS0051.E04, INF-16-000077, release date: 2016-04-22).
- **OpenScape Voice V9: Install V9 R0.8.3 Images (V9.00.01.ALL.12_PS0008.E03, INF-16-000200, release date: 2016-04-28).**

**3. Unify Application Server Products:**
The glibc library on Unify application servers should be patched at the earliest opportunity, as the overall risk cannot be determined by us. A timely update ensures that the whole operating system will be covered, as well as any third-party application that may coexist on the same server (Antivirus software, Monitoring agents etc.)
The following patch information is available:

- SUSE Linux Enterprise Server: CVE-2015-7547 (release date: 2016-02-16)
- Debian Linux: CVE-2015-7547 (release date: 2016-02-16)

We recommend to restart the servers after an update has been applied. This ensures that no application or service is still using the old version of the glibc library.
*Note that in very rare cases, applications may be statically linked to a vulnerable version of glibc at compile time. Those applications have to be recompiled (the operating system updates for glibc only cover all applications that dynamically link to glibc). If in doubt contact the vendor(s) of your 3rd-party application(s).*
*Unify products link dynamically and are therefore covered by the operating system updates.*

In case of virtualized installations of Unify application servers (on ESXi): Also consider the information provided by VMware Security Advisory VMSA-2016-0002.

## References

- NIST/NVD vulnerability entry: CVE-2015-7547
- GNU glibc: Vulnerability disclosure
- Google Security Team: Blog post
- FIRST: Common Vulnerability Scoring System (CVSS), V3

3rd Party Software - Fix release information:

- SUSE: CVE-2015-7547
- Debian Linux: CVE-2015-7547
- GNU glibc: Release information version 2.23
- VMware: VMSA-2016-0002

## Revision History

2016-02-19: Initial release
2016-02-25: Update 01

- Completed analysis for Unify products: added OpenStage Xpert 6010p (affected) and OpenScape Alarm Response (OScAR) Eco and Pro (not affected)
- Added release information for OpenStage Xpert 6010p and outlook to availability of fix releases for OpenScape 4000 Softgate and OpenScape Branch/SBC
- Added reference to Security Advisory by VMware

2016-03-08: Update 02

- Fix release available for OpenScape Branch and OpenScape SBC V7 R1;
  added note regarding recommended upgrade to V8 R1 or later

2016-03-15: Update 03

- Fix release available for OpenScape Branch, OpenScape SBC and Circuit Premise Universal Telephony Connector V8 R1
- Hotfix release available for HiPath 4000 V6 R2 and OpenScape 4000 V7 R1;
  added note regarding recommended upgrade to V7 R2
- Added clarification that only Linux-based OpenStage Xpert 6010p were affected (not the Windows-based)

2016-03-25: Update 04

- Fix release available for OpenScape Contact Center Call Director SIP Service (CDSS)
- Fix release available for OpenScape Voice V8 R1

2016-04-11: Update 05

- Fix release available for OpenScape 4000 V7 R2

2016-04-25: Update 06

- Fix release available for OpenScape Voice V7 R1

2016-04-29: Update 07

- Fix release available for OpenScape Voice V9

---

Advisory ID: OBSO-1602-02 (a=136), status: update 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