Security Advisory Report - OBSO-1501-04

GNU glibc Remote Buffer Overflow Vulnerability in gethostbyname - "Ghost" (CVE-2015-0235)

Creation Date: 2015-01-31
Last Update: 2016-10-10

Summary

On January 27, 2015, a vulnerability in the GNU glibc library (a core library used on Linux-based systems) was disclosed that affects many Linux-based systems worldwide. It has been assigned the vulnerability ID **CVE-2015-0235** and is also known as "**Ghost**" vulnerability.

This advisory summarizes the impact of CVE-2015-0235 for customers using products of Unify.

Risk for Unify products: low or none
See the product-specific details in the section "Affected Products" below.

Update 2015-02-11: Risk analysis for all Unify products completed.
Update 2016-10-10: Fix releases are now available for all affected Unify products.

Vulnerability Details

Researchers at Qualys identified a buffer overflow vulnerability in the GNU glibc library in versions 2.2 to 2.17 as used on many Linux-based systems. The vulnerability is located in library function called __nss_hostname_digits_dots() function and affects the gethostbyname() and gethostbyname2() functions in glibc. These functions are used in many applications and services of any type to resolve a hostname (such as "www.unify.com" or "myopenscapevoice.mycompany.de") to an IPv4 address.

Basically, a remote attacker could potentially exploit this vulnerability in two ways:

- **DoS (Denial of Service)**: the attacker sends arbitrary data to an application that overwrites the application's memory in a way that leads to a crash or restart of the application
- **RCE (Remote Code Execution)**: the attacker sends specially crafted data to an application to inject code and trigger its execution in the context of this application, or to obtain sensitive information from the application's memory, or a combination of both

Many different attack vectors may potentially exist on a system due to the widespread use of glibc in Linux-based operating systems, applications and services. Therefore, no exhaustive list of vulnerable applications could be compiled.
However, exploitation is limited by various mitigating factors. The following preconditions must apply for an individual application to be vulnerable:

- The application accepts hostnames as input from untrusted sources and resolves them by using a vulnerable gethostbyname*() function
- It does not perform data sanitization on the received hostname before calling gethostbyname*()
  (a malformed hostname needs to consist of more than 1000 Characters length, while the size of a host's full domain name according to IETF RFC 2181 is limited to 255 characters only)
- The input data an attacker can use for an exploit is limited to digits (0..9) and up to three dots (.) only and the buffer overflow is limited to 4 bytes (on 32-bit systems) or 8 bytes (on 64-bit systems) only
- The individual architecture of an application is crucial to determine whether an attack is feasible or not. There is no "one exploit fits all".

Affected Products

Unify has thoroughly checked its product portfolio for potential impact. Currently we assume that no Linux-based Unify product is vulnerable with significant risk.

The following tables list the result of the investigation in detail.

1. Embedded Devices and Software Appliances:
Wherever relevant, the correction of glibc will be included in the next fix or hotfix release of every individual product.

The Unify Product ...	uses vulnerable glibc	calls gethostbyname()	accepts remote input	is vulnerable to DoS?	is vulnerable to RCE?	Risk level	Solution - Update product to version (release date), or any later version:	Remarks
1.1 OpenScape Voice / Branch / SBC								
OpenScape Voice	yes	yes	no	no	no	low	V8 R0.34.4 (2015-03-06) V7 R1.42.2 (2015-03-11)	**Confirmed** vulnerable, but not exploitable (residual risk: low)
OpenScape Branch	yes	yes	yes	no	no	low	V8 R0.27.0 (2015-02-09) V7 R1.27.0 (2015-03-06)	**Confirmed** vulnerable, but not exploitable (residual risk: low)
OpenScape SBC	yes	yes	yes	no	no	low	V8 R0.27.0 (2015-02-13) V7 R1.27.0 (2015-03-06)	**Confirmed** vulnerable, but not exploitable (residual risk: low)
1.2 HiPath 4000 V6 / OpenScape 4000 V7								
Softgate	yes	yes	yes	no	no	low	V7 R1.8.5 (2015-02-20) V6 R2.17.2 (2015-02-20)	**Confirmed** vulnerable, but not exploitable (residual risk: low)
Assistant	yes	yes	yes	no	no	low	V7 R1.7.5 (2015-03-18) V6 R2.51.3 (2015-04-22)	**Confirmed** vulnerable, but not exploitable (residual risk: low)
CSTA	yes	yes	yes	no	no	low	V7 R1.206.5 (2015-04-24) V6 R2: V1 R13.204.2 (2015-03-26)	**Confirmed** vulnerable, but not exploitable (residual risk: low)
Platform	yes	yes	no	no	no	info	V7 R1.39.0 (2015-05-29)	**Confirmed** not vulnerable (but fix release provided as a precautionary measure)
1.3 OpenScape Business / OpenScape Office								
OpenScape Business	yes	yes	yes	no	no	low	V2 R0.2.0 (2015-07-17)	**Confirmed** vulnerable, but not exploitable (residual risk: low)
OpenScape Office	yes	yes	yes	no	no	low	**V3 R3.14.0 (2016-08-10)**	**Confirmed** vulnerable, but not exploitable (residual risk: low)
1.4 OpenStage / OpenScape Desk Phone IP (SIP and HFA)								
35G Eco SIP V3 R3	yes	yes	yes	yes	no	low	V3 R3.36.0 (2015-04-10)	**Confirmed** vulnerable to DoS and not vulnerable to RCE. (*)
OpenStage / OpenScape Desk Phone IP, all other models	no	n.a.	n.a.	no	no	info	n.a.	**Confirmed** not vulnerable
1.5 Further Products								
OpenScape Contact Center CDSS	yes	yes	no	no	no	info	**V8 R2.10.11192 (2015-07-24)**	**Confirmed** not vulnerable (but fix release provided as a precautionary measure)
HiPath Cordless IP	no	n.a.	n.a.	no	no	info	n.a.	**Confirmed** not vulnerable
OpenScape Alarm Response Eco and Pro	yes	no	n.a.	no	no	info	n.a.	**Confirmed** not vulnerable

(*) Arbitrary remote input via the DLS-WPI may lead to DoS (reboot of the phone). The exploit requires authentication as per configured security level (Default Mode or Secure Mode). Therefore, no significant additional risk, as the reboot can be initiated in the same DLS-WPI session context in a legitimate way.

2. Applications:
The Unify applications listed below run on Linux application servers (SUSE Linux Enterprise Server or Debian Linux) that comes with a potentially vulnerable version of glibc. The given risk estimation relates to the potential attack vectors that the Unify application adds. It does not include the potential additional vectors of the underlying operating system services or 3rd-party applications installed on the same server. Updates for vulnerable server operating systems are available and should be applied as soon as possible. See chapter 2. in the section "Recommended Actions" for details.

The Unify Product ...	calls gethostbyname()	accepts remote input	is vulnerable to DoS?	is vulnerable to RCE?	Risk level	Solution - Apply patch for:	Remarks
2.1 OpenScape UC Application Servers							
Frontend, Backend, Facade	no	n.a.	no	no	info	SUSE SLES	**Confirmed** not vulnerable
Media Server	yes	no	no	no	info	SUSE SLES	**Confirmed** not vulnerable
Common Management Platform (CMP)	yes	no	no	no	info	SUSE SLES	**Confirmed** not vulnerable
2.1 Further Linux-based applications							
OSV Survival Authority	no	n.a.	no	no	info	SUSE SLES	**Confirmed** not vulnerable
HiPath / OpenScape 4000 Manager	yes	no	no	no	low	SUSE SLES	**Confirmed** vulnerable, but not exploitable (residual risk: low)
OpenScape Business S and UC Booster Server	yes	no	no	no	low	SUSE SLES	**Confirmed** vulnerable, but not exploitable (residual risk: low)
OpenScape Xpert Multi-Line Control server (MLC)	yes	no	no	no	low	Debian Linux (wheezy)	**Confirmed** vulnerable, but not exploitable (residual risk: low)

Recommended Actions

The table in the section "Affected Products" should help customers to determine the overall risk in their individual deployment and to prioritize and schedule the associated updates of the operating systems and Unify products.
The table will be updated as soon as new information is available.

1. Embedded Devices and Software Appliances
As a precautionary measure, any Unify product should be updated, as soon as an associated fix or hotfix release is available.

2. Applications
glibc 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-2015-0235 (release date: 2015-01-28)
- Debian 7 (wheezy): CVE-2015-0235 (release date: 2015-01-27)

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.

References

Description of the "ghost" vulnerability:

- Qualys Security Advisory
- Qualys Blog: The GHOST vulnerability

Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235
NVD: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0235

Solutions for Application Servers:

- SUSE Linux Enterprise Server: CVE-2015-0235 (release date: 2015-01-28)
- Debian 7 (wheezy): CVE-2015-0235 (release date: 2015-01-27)

Revision History

Undone draft changes to rerelease latest released version for the LE-Split History

2015-01-31: Initial release
2015-02-11: Update 01

- Risk analysis completed; overall risk for Unify products reduced from "medium" to "low"
- Updated table with latest analysis results for affected Unify products
- Added release information for OpenScape Branch V8 and upcoming release plans where available

2015-02-14: Update 02

- Added release information for OpenScape SBC V8

2015-03-11: Update 03

- Updated risk analysis for OpenScape Contact Center CDSS (confirmed as not vulnerable)
- Added release information for OpenScape Voice V8 and for OpenScape Voice, OpenScape Branch and OpenScape SBC V7 R1
- Added release information for HiPath 4000 V6 R2 / OpenScape 4000 V7 R1 Softgate

2015-05-08: Update 04

- Added release information for OpenStage / OpenScape Desk Phone IP 35G Eco SIP
- Added release information for HiPath/OpenScape 4000 Assistant and CSTA

2015-05-29: Update 05

- Added release information for OpenScape 4000 V7 R1 Platform

2015-07-28: Update 06

- Added release information for OpenScape Business and for OpenScape Contact Center CDSS

2016-10-10: Update 07

- Added release information for OpenScape Office V3 R3
  With this update, fix releases are now available for all affected Unify products.

Advisory ID: OBSO-1501-04 (a=102), 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