# Security Advisory Report - OBSO-1412-02

## NTP - Multiple Stack Based Buffer Overflow Vulnerabilities (CVE-2014-9295)

Creation Date: 2014-12-23
Last Update: 2015-01-27

## Summary

On December 19, 2014, multiple vulnerabilities were disclosed for the network time protocol daemon (ntpd) on Linux servers. They could allow remote attackers to cause a denial of service (DoS) of the ntp service or to execute arbitrary code of the system where the ntp service is running on.

This advisory summarizes the impact of the vulnerability for customers using products of Unify and the recommended countermeasures.

The risk is rated as medium for older versions of HiPath/OpenScape 4000 Assistant and CSTA.
**As of 2015-01-27, investigation has completed and no risk for other Unify products has been identified.**

## Vulnerability Details

Network Time Protocol (ntpd daemon versions before 4.2.8) is prone to three stack-based buffer-overflow vulnerabilities because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

Specifically, the issues affect the functions crypto_recv() (when the Autokey Authentication feature is used), ctl_putdata() and configure() of the "ntpd" daemon. The vulnerabilities could be exploited by sending specially crafted packets via the ntp port (udp/123) to a vulnerable "ntpd" daemon.

Successful exploits may allow an attacker to execute arbitrary code with the privilege level of the ntpd process. Failed attempts will likely cause a denial-of-service condition.

## Affected Products

**1. Vulnerable with medium risk**

- **HiPath 4000 Assistant** before V6 R2.42.4
- **HiPath 4000 CSTA** in HiPath 4000 V6 R2: CSTA versions before V1 R13.203.1
- **OpenScape 4000 Assistant** before V7 R0.14.5
- **OpenScape 4000 CSTA** before V7 R0.205.3

Older versions of Assistant/CSTA have the ntpd service enabled in a configuration that potentially allows remote code execution on the Linux system of Assistant or CSTA; the risk is rated as medium:
CVSS Base Score: 5.1, CVSS Temporal Score: 4.1
CVSS v2 Vector (AV:N/AC:H/Au:N/C:P/I:P/A:P/E:U/RL:W/RC:C)

Current versions of Assistant and CSTA (in both HiPath 4000 V6 R2 and OpenScape 4000 V7 R0/R1) have removed the ntp service and are therefore not vulnerable.

**2. Vulnerable with low risk**

- none

**3. Not vulnerable**

Other Linux-based Unify products are not affected for different reasons:

- the ntpd service in not in use (but ntp client functions only), as e.g. in OpenStage / OpenScape Desk Phone IP, HiPath Cordless IP, OpenStage WL3 phones and WSG, or HiPath/OpenScape 4000 Assistant/CSTA (latest versions)
- the ntpd service is not exposed remotely, as e.g. in HiPath/OpenScape 4000 Platform
- the ntpd service is hardened by default in a way that prevents exploitability, as e.g. in OpenScape Voice, OpenScape Branch, OpenScape SBC, OpenScape Business or OpenScape Office

## Recommended Actions

Install the following Unify product releases (or later versions) to resolve the vulnerability:

- **HiPath 4000 V6**:
    - Assistant: V6 R2.42.4 (release date: 2014-07-25)
    - CSTA: V1 R13.203.1 (release date: 2014-06-06)
- **OpenScape 4000 V7**:
    - Assistant: V7 R0.14.5 (release date: 2014-07-15)
    - CSTA: V7 R0.205.3 (release date: 2014-06-06)

**Recommendation for Linux-based applications of Unify**
(such as OpenScape UC application servers, Media Server, Common Management Platform, OpenScape 4000 Manager, OpenScape Business S/Booster Server, OpenScape Office LX/HX, OpenScape Xpert System Manager):

- Applications installed on SUSE Linux Enterprise Server: apply the hardening recommendations as provided by SUSE (https://www.suse.com/security/cve/CVE-2014-9295.html)
- Applications installed on Debian Linux (OpenScape Xpert Multi Line Controller only): apply the hardening recommendations as provided by Debian (https://security-tracker.debian.org/tracker/CVE-2014-9295)
- ntp.org provides a comprehensive guide for secure operation of NTP servers at: http://support.ntp.org/bin/view/Support/AccessRestrictions

## References

External links:

- ntp.org: Security Notices for CVE-2014-9295 et. al. and ntpd Access Restrictions
- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9295
- NVD: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9295
- US-CERT: http://www.kb.cert.org/vuls/id/852879

Patch information for Operating Systems:

- SUSE Linux Enterprise Server: https://www.suse.com/security/cve/CVE-2014-9295.html
- Debian Linux: https://security-tracker.debian.org/tracker/CVE-2014-9295

## Revision History

2014-12-23: Initial release
2015-01-27: Update 01

- Investigation completed for Unify products
- Moved OpenScape Business to the list of not affected products

Advisory ID: OBSO-1412-02 (a=100), 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

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.