Security Advisory Report - OBSO-1610-03

Leap Second on 2016-12-31 - Security Note for Unify Products

Creation Date: 2016-10-27
Last Update: 2016-10-27

Summary

The International Earth Rotation & Reference Systems Service announced the **introduction of a new leap second** for the Coordinated Universal Time (UTC) **at the end of December, 2016** to correct differences between astronomical and atomic time caused by irregularities of earth rotation *(Ref: The last Bulletin C at the* Earth Orientation Center*).*
This event does not constitute a security vulnerability, but could cause system outages or service interruptions due to the exceptional handling of leap seconds in computer systems.

The Security Note summarizes the impact of this leap second on Unify products and recommended actions.
The overall risk for potential system outages or service interruptions in Unify products is rated as low.

Vulnerability Details

A positive leap second will be introduced between December 31, 2016, 23h 59m 59s and January 1, 2017, 0h 0m 0s UTC.
All NTP servers supporting Network Time Protocol version 4 according to IETF RFC 5905 and attached to an appropriate NTP time service (or configured otherwise according to the current version of the List of Leap Seconds provided by US NIST) will receive a leap second indicator during the month of December. This will be propagated to NTP clients (e.g. any Linux or Windows system kernel) somewhen (unpredictable) during the day when the leap second has to be added to the system clock. The system kernel will then add this extra second to the system clock at the end of the day (after December 31, 23h 59m 59s UTC).
The following issues are known which could potentially impact system stability or availability:

1. **Windows time service**: no issues are known; there is no impact expected on applications running on Windows (client or server) operating systems
2. **Linux kernel versions 2.6.26 through 3.3**: a bug in the handling of timers (due to a missing "clock was set" event during the leap second) could cause a system to consume up to 100% CPU time
3. **SUSE Linux Enterprise Server (SLES) 11 SP1 - SP3**: an incomplete fix for issue #2 could cause a kernel deadlock and freeze the system. Systems running on SLES 11 SP4, SLES 12 or higher are not affected by #2 or #3.
4. **SUSE Linux Enterprise Server (SLES), all versions prior to 12 SP2**: Absolute timers that expire at Midnight UTC may fire early when the Leap Second is inserted.

The following chapters refer to these four different issues accordingly (*"Regarding 1./2./3./4."*)

Affected Products

Regarding 1: No impact is expected on Unify products running on Microsoft Windows operating systems

Regarding 2: Impacted with low risk:

- OpenScape Office MX - all versions up to and including V3 R3

Regarding 3: Impacted with low risk:

- Unify Server Applications (e.g. OpenScape Voice Survivability Authority, UC Application servers, OpenScape 4000 Manager, any other Management application, OpenScape Business S and Booster Server), but only if still running on SUSE Linux Enterprise Server 11 SP3 or earlier.
  Note that the use of SLES 12 or SLES 11 SP4 as application platform is preferred and recommended anyway. See also Security Advisory OBSO-1603-01.

Regarding 4: No impact is expected on Unify Server Applications running on SLES 11 or 12 or on Unify, or on Unify appliances based on SLES or openSUSE.

Recommended Actions

Important general notes:

- **Products that are not connected to an NTP service** are not affected by the leap second event. As the drift for unsynchronized clocks is typically greater than one second, we also do not recommend any manual interaction to adjust the time because of the leap second event
- **No Unify-internal test was able to produce any negative impact** on any Unify product stability or availability associated with the leap second event. The residual risk for customer installations without having applied the recommended actions is rated as low. Therefore, in cases where the recommended actions can not be performed, the following alternative action can be considered:
  "Do nothing", but check system status after the leap second has passed. In the (unlikely) event of service outages, restart the affected servers one by one according to the individual product procedure.

Regarding 2:

- **OpenScape Office MX:**
  Temporarily deactivate NTP configuration via the product's standard configuration interface and reactivate it on January 1st or afterwards. The deactivation of the NTP synchronisation for a few days does not impact system stability.

Regarding 3:

- **Unify Applications running on SUSE Linux Enterprise Server before SLES 11 SP4:**
  - Update the operating system to SLES 11 SP4 or 12.
  - Follow the recommendations provided by SUSE at: https://www.suse.com/support/kb/doc.php?id=7016150

Notes for installations with Unify products that already achieved end of SW support:
A higher risk of potential outages can be expected for:

- **OpenScape Contact Center Call Director SIP Service (CDSS) before V8 R2.10** (release date: 2015-07-25). See Security Advisory OBSO-1508-01.
  Solution: Update to V9 R0.2.0 or any later version.
  Note: CDSS V9 is compatible with both OpenScape Contact Center V8 and V9 installations.
- **HiPath 4000 V6 R1 Softgate and Platform, before V6 R1.12.2** (HF003013, release date: 2012-11-29).
  Solution: Upgrade to OpenScape 4000 V7 R2, latest version
  Note: The OpenScape Baseline Security Office considers the risk of malicious attacks against HiPath 4000 V6 before V6 R1.12.2 as significantly higher than an accidental temporary outage caused by the insertion of the leap second. Refer to Security Advisory OBSO-1409-01 as one major example. We therefore recommend customers who are still on outdated versions of OpenScape 4000 to upgrade, independent of the upcoming leap second event.

For more information regarding Unify product versions that are beyond end of SW support, refer to the Security Advisory OBSO-1505-01. This advisory also lists the relevant fix releases where additional measures were taken in the past to prevent from potential outages.

References

External References:

- Bulletin C at the Earth Orientation Center
- Network Time Protocol Version 4: IETF RFC 5905
- SUSE Knowledgebase article: https://www.suse.com/support/kb/doc.php?id=7016150

Related Unify Security Advisories:

- OBSO-1409-01 - Bash - Remote Command Injection Vulnerability "Shellshock" (CVE-2014-6271, CVE-2014 7169 et al.)
- OBSO-1505-01 - Leap Second on 2015-06-30 - Security Note for Unify Products
- OBSO-1508-01 - OpenScape Contact Center CDSS - Multiple vulnerabilities fixed in V8 R2.10.11192
- OBSO-1603-01 - Unify SLES 11-based Server Applications - Support of SLES 11 SP4

Revision History

Initial release: 2016-10-27

Advisory ID: OBSO-1610-03 (a=149), 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