unify

Security Advisory Report - OBSO-1408-04

Java in Unify products - RSA private key timing attack vulnerability (CVE-2014-4244) and failure to validate public Diffie-Hellman parameters (CVE-2014-4263)

Creation Date:	2014-08-26
Last Update:	2015-08-21

Summary

In the context of the July 2014 Oracle Patch Day (2014-07-15), 20 new (partially high risk) security vulnerabilities for Oracle Java SE (Java Runtime Environment - "JRE") were disclosed.
The product portfolio of Unify is potentially and directly impacted by only two of the reported vulnerabilities. They are rated as follows:

- Low risk: RSA private key timing attack vulnerability (CVE-2014-4244)
- Low risk: Failure to validate public Diffie-Hellman parameters (CVE-2014-4263)

The associated updates in affected products will be included as part of their regular release cycle.

Furthermore this Security Advisory provides additional recommendations regarding the use of Oracle JRE on end-user devices (client deployments of the JRE).

Vulnerability Details

Although the vulnerabilities were reported for Oracle Java, they partially also affect the IBM Java components as delivered with Unify products:

1. CVE-2014-4244 (RSA private key timing attack vulnerability):

The RSA algorithm in the Security component in Java did not sufficiently perform blinding while performing operations that were using private keys. A remote attacker able to measure timing differences of those operations could possibly leak information about the used keys.

Mitre (cve.mitre.org) has assigned the id CVE-2014-4244 to this issue.
CVSS v2 Base Score for Unify products: 3.2 (AV:A/AC:H/AU:N/C:P/I:P/A:N)

2. CVE-2014-4263 (Failure to validate public Diffie-Hellman parameters):

The Diffie-Hellman (DH) key exchange algorithm implementation in the Java Security component failed to validate public Diffie-Hellman parameters properly. This could allow the Java implementation to accept and use weak parameters, making it possible for attackers to recover the negotiated key.

Mitre (cve.mitre.org) has assigned the id CVE-2014-4263 to this issue.
CVSS v2 Base Score for Unify products: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

3. Note regarding Oracle Java Runtime Environment (JRE) on end-user devices:

All 20 reported vulnerabilities are potentially relevant to installations of Oracle JRE on end-user devices (client deployments of JRE, such as Java plug-in in Browsers or Java WebStart applications).
Unify recommends to follow the advise from Oracle and keep these installations up-to-date with the latest version of Oracle JRE (as available on: http://www.java.com/en/download/manual.jsp; currently this is **version 8 Update 60**).
So far there are no known limitations or incompatibilities known when this update is used together with Java clients provided by Unify products. For details refer to the *Handling of Oracle JRE on end-user devices* in chapter "Recommended Actions" below.

Affected Products

Three Unify products were identified as affected with low risk:

- OpenScape UC Applications, **all versions before V7 R3.0.0**
- OpenScape Voice (integrated simplex variant only), **all versions before V8 R0.34.4 and V7 R1.42.2**
- OpenScape/HiPath 4000 (Softgate only), **all versions before V7 R1.39.0 and V6 R2.17.0**

The updates in affected products have been provided as part of the regular release cycle (see below.)

Recommended Actions

CVE-2014-4244 and CVE-2014-4263:

Install the corresponding product updates or any later released version as follows:

- OpenScape UC Applications: V7 R3.0.0 (release date: 2015-07-24)
- OpenScape Voice (integrated simplex):
  - V8 R0.34.4 (release date: 2015-03-06)
  - V7 R1.42.2 (release date: 2015-03-11)
- OpenScape/HiPath 4000 Softgate:
  - V7 R1.39.0 (release date: 2015-05-29)
  - V6 R2.17.0 (release date: 2014-12-11)

Handling of Oracle Java Runtime Environment (JRE) on end-user devices:
This description only applies to Unify products where Java applets or web-start applications are provided for use on end-user devices (such as the Web-based User Interface of OpenScape Deployment Service, OpenScape User Management, or OpenScape 4000 Manager/Assistant) and therefore require the existence or prior installation of Oracle JRE on these devices:

- Oracle Java Runtime Environment (JRE) is always installed by the user/customer, Unify products do not deliver it
- From a Unify product's perspective, there is - by default - no restriction for the users/customers to keep the JRE up-to-date with latest versions as released by Oracle
- In practice it may happen, that the latest JRE version is incompatible with one or more applets or Web-Start applications as provided by products of Unify
  In such intermediate situations a downgrade to an older JRE version may be advisable to avoid that customers working with the affected product's graphical user interface are not blocked. However, all applications running on an end-user device are constantly target of attacks and JRE is no exception here. Therefore, before downgrading to an older version the following should be taken into consideration:
  - what the end-user device's environment is (for example: is it a general purpose PC, also surfing the internet - or admin only PC in a restricted network?)
  - what known and open vulnerabilities the customer's end-user device is enfaced with, when operating an outdated version of the JRE
- Customers should report the problem to Unify using the normal product support process
- As soon as such type of incompatibilities become known, Unify Product Development analyses them and resolves them with appropriate priority. Usually a correction is provided as part of a fix or hotfix release to resolve this intermediate situation for all customers

References

External links:

- Oracle: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html#AppendixJAVA
- IBM: http://www.ibm.com/developerworks/java/jdk/alerts/#Oracle_July_15_2014_CPU
- Novell: https://support.novell.com/security/cve/CVE-2014-4244.html and https://support.novell.com/security/cve/CVE-2014-4263.html

Revision History

2014-08-26: Initial release

2015-08-20: Update 01

- Included release information for all affected products (OpenScape Voice, OpenScape/HiPath 4000 Softgate, OpenScape UC Applications)
- Java on end-user devices: updated information about currently latest and recommended version (Oracle JRE 8 update 60)

Advisory ID: OBSO-1408-04 (a=86), 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.