Security Advisory Report - OBSO-1511-01

Deserialisation of Java-objects - Vulnerability in Applications involving Apache Commons-Collections Classes (CVE-2015-8237, CVE-2015-8238)

Creation Date:	2015-11-17
Last Update:	2016-01-22

Summary

Java applications that contain Apache Commons Collections classes (such as the InvokerTransformer class) in their classpath may be vulnerable to arbitrary remote code execution if untrusted data is deserialized.
This is a vulnerability as defined in CWE-502.

This advisory summarizes the impact for Java-based application products of Unify and provides associated recommendations how to mitigate and solve the issue.

Unify products are considered vulnerable as follows:

- **High risk** for OpenScape Fault Management (CVE-2015-8237)
- **Medium risk** for certain OpenScape UC Application Servers (CVE-2015-8238)
- **Hardening information** available for OpenScape Common Management Platform (CMP) (CVE-2015-8238)
- Other Unify products are considered as not vulnerable

Vulnerability Details

On November 6, 2015 security researchers released zero day exploits for various Java applications, leveraging unsafe deserialization of Java objects in the InvokerTransformer class of Apache Commons Collections. Successfully exploiting this issue could allow remote attackers to execute arbitrary code in the context of the affected application.
A comprehensive description of the issue is available at the researchers' site and the Vulnerability Note VU#576313 by CERT/CC.

The risk for Unify products depends on the individual product's implementation and is listed in the "Affected Products" section.

Mitre has assigned the CVE-IDs CVE-2015-8237 for OpenScape Fault Management and CVE-2015-8238 for both OpenScape UC Application and Common Management Platform.

Affected Products

1. OpenScape Fault Management V7 (before V7 R0.73.13) and V8 (before V8 R0.63.3):
The Fault Management RMI ports 3042/tcp and 3050/tcp (Client-Server ports) and 3040/tcp, 3049/tcp, 3060/tcp (Event Gateway) potentially allow a remote attacker to execute arbitrary code with elevated privileges on the Fault Management server.
Fix releases are in work for all actively sustained versions (V7, V8). The upcoming new version V9 (currently in field trial status) will have the fix included in its first GA (General Availability) release.
The advisory will be updated as soon as the fix releases are available.
We recommend to apply the mitigation measures listed in the section "Recommended Actions".

Risk: high
CVSSv3 Scores: Base Score 9.8, Temporal Score 8.7
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:W/RC:C)

2. OpenScape UC Application, all versions:
The js-soc protocol on port 4711/tcp (or alternatively, if TLS is used: 4710/tcp) potentially allow a remote attacker to execute arbitrary code with user-level privileges on Media Server, Frontend Server or Backend Server instances within a UC Application deployment.
A fix release is in work for the actively sustained version (V7 R3). The advisory will be updated as soon as the fix release is available.
We recommend to apply the mitigation measures listed in the section "Recommended Actions".

Risk: medium
CVSSv3 Scores: Base Score 6.3, Temporal Score 5.6
(CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:W/RC:C)

3. OpenScape Common Management Platform (CMP), all versions:
The interfaces/ports listed in 2. above, are also used by CMP, but for local use only **in CMP standalone installations.** (For CMP in UC installations, refer to 2. above.)
We recommend to apply the mitigation measures listed in the section "Recommended Actions".

Note: the following Unify products also contain Java code, but are confirmed as not vulnerable:

- ***Android Mobile Apps**: Circuit, OpenScape Mobile, OpenScape Web, myPortal to go, Contact Center Supervisor*
- ***Server Applications**:OpenScape UC: Facade Server and Openfire, OpenScape Xpressions, OpenScape Business S, Booster Server, OpenScape Contact Center Extensions (OSCC-E) and Campaign Director*
- ***Management Applications**: OpenScape Deployment Service (DLS), OpenScape User Management (UM), OpenScape Quality of Service Management (QM), HiPath/OpenScape 4000 Manager, SESAP*
- ***Communication Platforms**: OpenScape Voice, OpenScape Branch, OpenScape SBC, HiPath/OpenScape 4000 (incl. Platform, Softgate, CSTA, Assistant), OpenScape Business, OpenScape Office*

Recommended Actions

Fix Releases:

- OpenScape Fault Management V8: install Hotfix V8 R0.63.3 (HF004306, release date 2015-11-25) or any later version
- OpenScape Fault Management V7: install Hotfix V7 R0.73.13 (MSC26980, release date 2015-12-07) or any later version
- OpenScape UC Application and Common Management Portal: **upgrade to V7 R3.0.7 (**HF004353**, release date 2016-01-22) or any later version**

Mitigation Measures:
The following settings are recommended as general best-practice security hardening in the customer's network - regardless if a fix for this particular issue in the affected Unify product(s) is installed or not.

1. OpenScape Fault Management:
Apply appropriate firewall settings and other access control configuration as follows:

- The ports **3042/tcp and 3050/tcp** are used for Fault Management client to server communication. Limit access to these server ports from trusted systems only; preferably they should only be accessible from dedicated clients in a restricted administration network. Apply appropriate firewall settings using the operating system's built-in capabilities of the server where Fault Management runs on (Windows server or Linux server)
- The ports **3040/tcp, 3049/tcp, 3060/tcp** are associated with the Event Gateway (MEG) and are affected as well. The ports are only used locally on the Fault Management server. Configure the firewall rules accordingly to allow localhost communication only.
  In V7, the Event Gateway may optionally also be installed on a separate server aside of the Fault Management server; if this is the case, restrict the communication accordingly to allow connections only between these two servers.

In deployments where System Management Agents are deployed on remote hosts, you could add these hosts to the list of trusted systems in the Fault Management server's firewall configuration as above. The recommended solution however is to block these systems; the Fault Management server will automatically switch to an unidirectional mode and consecutively poll the Agents through a port that is not vulnerable.

2. OpenScape UC Application:
A UC Application deployment is only potentially attackable from inside the security zone of UC servers, i.e. where access on IP address level is possible to the listener **port 4711/tcp (or alternatively, if TLS is used: 4710/tcp)** on Media Server (MS), Frontend Server (FE) or Backend Server (BE). **There are two options to prevent potential misuse:**

- If the network where all UC Servers are located is already considered trusted and appropriate measures have been taken to prevent unauthorized systems to access this network: no further measures are neccessary
- In all other cases: apply appropriate firewall settings using the SUSE Linux Enterprise Server operating system's built-in capabilities (iptables) to restrict traffic from/to these ports to the servers (MS, FE, BE) involved in your UC deployment. All UC servers should be able to send and receive packets through the given ports only from/to all other UC nodes.

3. OpenScape Common Management Platform (CMP):
The ports **port 4711/tcp (or alternatively, if TLS is used: 4710/tcp)** are used only for local communication **in a CMP standalone deployment**. Configure the firewall rules accordingly to allow localhost communication only. **For CMP in a UC deployment, the configuration rules apply as outlined in 2. above.**

References

- Initial security researcher publication (2015-11-06)
- CERT/CC Vulnerability Note VU#576313
- NIST/NVD vulnerability entries:
  - CVE-2015-8237
  - CVE-2015-8238
- CWE-502: Deserialization of untrusted data

Revision History

2015-11-17: Initial release
2015-11-18: Update 01

- No significant change in current content, but use of correct CVE IDs as assigned by Mitre

2015-11-26: Update 02

- Fix release available for OpenScape Fault Management V8
- Corrected typo in product name (Common Management *Portal* --> *Platform*)

2015-12-08: Update 03

- Fix release available for OpenScape Fault Management V7
- Recommended Actions: Clarification of the difference between CMP standalone and CMP in UC Deployments; more details regarding the secure operation of UC servers

2016-01-22: Update 04

- Fix release available for OpenScape UC Application and Common Management Platform

Advisory ID: OBSO-1511-01 (a=123), 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.