Security Advisory Report - OBSO-1512-04

Apache Tomcat Denial of Service Vulnerability in ChunkedInputFilter (CVE-2014-0227)

Creation Date:	2015-12-30
Last Update:	2016-01-22

Summary

The Apache Tomcat component as included in various Unify products contains a vulnerability that could allow an unauthenticated, remote attacker to perform a denial of service attack against the product's web based interfaces (https or http).

The risk is rated **medium**.

The issue is caused by a flaw in the ChunkedInputFilter class of Apache Tomcat that may lead to HTTP request smuggling or denial of service attacks as documented in CVE-2014-0227 and in the the Security Reports for Apache Tomcat 6 or Tomcat 7.

This advisory lists the affected versions of Unify products and associated recommended actions.

Vulnerability Details

Denial of Service:
When Chunked Transfer Encoding is used in HTTP/1.1 connections, the ChunkedInputFilter implementation in Tomcat does not abort subsequent attempts to read input after a failure occurred. A remote attacker could utilize this flaw by sending malformed chunked requests and streaming an unlimited quantity of data. This could lead to a denial of service condition by excessive consumption of server resources at the https (or http) interfaces of various Unify products as listed below.

HTTP Request Smuggling:
The vulnerability could also leverage HTTP request smuggling attacks. However, this could not be confirmed for any of the listed Unify products.

Mitre has assigned CVE-2014-0227 to this issue in Apache Tomcat. Further information is available in the Security Reports for Apache Tomcat 6 or Tomcat 7.

CVSSv3 scores for Unify Products:

- Base Score: 5.3 (Medium)
- Temporal Score 4.6 (Medium)
- CVSS v3 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:U/RL:O/RC:C)

Affected Products

Products confirmed as vulnerable
(in brackets: list of affected https and http ports, where Apache Tomcat is listening on):

- OpenScape UC Application:
  - Web Client interface on Frontend Server *(https on 8443/tcp or http on 8081/tcp)*
  - Facade Server *(https on port 8443/tcp, or http on 8081/tcp)*
- OpenScape Common Management Platform *(https on port 443/tcp)*
- OpenScape Deployment Service:
  - Administration interface (DLS Web GUI and API) *(https on ports 10443 and 10444 or http on port 18080)*
  - Workpoint interface (DLS-WPI) *(https on ports 18443 and 18444)*
- OpenScape License Management *(https on port 8818 or http on port 8819)*

Recommended Actions

Fix Releases:

- OpenScape UC Application: Upgrade to V7 R3.0.0 (release date: 2015-07-24) or any later version
- OpenScape Common Management Platform: **Upgrade to V7 R3.0.7 (release date: 2016-01-22) or any later version**
- OpenScape Deployment Service (DLS): Upgrade to V7 R3.0.0 (release date: 2015-06-01) or any later version (*)
- OpenScape License Management: Upgrade to V1 R16.0.0 (release date: 2015-10-27) or any later version

(*) The upgrade to DLS V7 R3.10.0 (release date: 2015-12-21) is recommended as it solves an additional denial of service vulnerability in Apache Tomcat (CVE-2014-0230). This issue is rated as low risk for the listed Unify products (CVSSv3 Base Score 3.7, Temporal Score 3.2) and is fixed in all other products (except DLS) with the same release as CVE-2014-0227.

Mitigation Measures:

- If network security solutions (such as IDS, IPS, SIEM or similar) are in place: monitor network traffic to identify and locate abnormally high HTTP traffic to the listed interface ports.

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.

- Apply suitable network configuration measures to restrict the access to the web based interfaces to authorized systems, devices and users only.

References

- NIST/NVD vulnerability entry: CVE-2014-0227
- CVE-2014-0227 in Apache Tomcat Security Reports for Tomcat 6 and Tomcat 7
- FIRST: Common Vulnerability Scoring System (CVSS), V3

Revision History

2015-12-30: Initial release
2016-01-22: Update 01

- Fix release available for OpenScape Common Management Platform

Advisory ID: OBSO-1512-04 (a=121), 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.