Security Advisory Report - OBSO-1805-01

Spring Framework spring-messaging Module Message Handling Remote Code Execution (CVE-2018-1270, CVE-2018-1275)

Creation Date: 2018-05-22 10:09:16
Last Update: 2018-06-01 14:08:25

Summary

Update #1:

Analysis showed that UC applications are not affected.

Spring Framework contains a flaw in the spring-messaging module that is triggered during the handling of a specially crafted message. This may allow a remote attacker to potentially execute arbitrary code.

Details

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 (CVE-2018-1270) / prior to 4.3.16 (CVE-2018-1275) and older unsupported versions allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack.

Vulnerable Spring Framework versions expose STOMP clients over WebSocket endpoints with an in-memory STOMP broker through the 'spring-messaging' module, which could allow an attacker to send a maliciously crafted message to the broker, leading to a remote code execution attack (CVE-2018-1270).

https://thehackernews.com/2018/04/spring-framework-hacking.html

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.16 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack. This CVE addresses the partial fix for CVE-2018-1270 in the 4.3.x branch of the Spring Framework. (CVE-2018-1275).

Affected Products

Unify products affected with a fix available:

Circuit Backend Services

Use Circuit Operations Node 1.10.96.0 or later.

Fix is available in Sprint 96

Circuit Clients:

Use Circuit Provisioning Agent 0.8.11 or later

Unify products affected with a fix in work

Composer

All other products are not affected because they either do not use Spring Framework or do not use Websockets.

Recommended Actions

For products affected:
Update to the latest version available.

References

https://spring.io/blog/2018/04/05/multiple-cve-reports-published-for-the-spring-framework

https://thehackernews.com/2018/04/spring-framework-hacking.html

https://www.us-cert.gov/ncas/bulletins/SB18-099

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-1270
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-1275

https://pivotal.io/security/cve-2018-1270
https://pivotal.io/security/cve-2018-1275

https://spring.io/blog/2018/04/03/spring-framework-5-0-5-and-4-3-15-available-now
https://spring.io/blog/2018/04/05/spring-boot-2-0-1-available-now

Advisory: OBSO-1805-01, 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

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.