Security Advisory Report - OBSO-1812-01

Spring Framework ResourceHttpRequestHandler Remote DoS (CVE-2018-15756)

Creation Date: 2018-12-10 14:15:45
Last Update: 2018-12-13 16:42:24

Summary

Spring Framework contains a flaw that is triggered during the handling of a specially crafted range header with a high number of ranges or wide ranges that overlap.
This may allow a remote attacker to cause a denial of service.

Details

Spring Framework, version 5.1, versions 5.0.x prior to 5.0.10, versions 4.3.x prior to 4.3.20, and older unsupported versions on the 4.2.x branch provide support for range requests when serving static resources through the ResourceHttpRequestHandler, or starting in 5.0 when an annotated controller returns an org.springframework.core.io.Resource.
A malicious user (or attacker) can add a range header with a high number of ranges, or with wide ranges that overlap, or both, for a denial of service attack.

This vulnerability affects applications that depend on either spring-webmvc or spring-webflux. Such applications must also have a registration for serving static resources (e.g. JS, CSS, images, and others), or have an annotated controller that returns an org.springframework.core.io.Resource.

Spring Boot applications that depend on spring-boot-starter-web or spring-boot-starter-webflux are ready to serve static resources out of the box and are therefore vulnerable.

Affected Pivotal Products and Versions

Severity is low unless otherwise noted.

- Spring Framework 5.1
- Spring Framework 5.0.0 to 5.0.9
- Spring Framework 4.3 to 4.3.19
- Older unsupported versions going back to 4.2 are also affected

Mitigation

Users of affected versions should apply the following mitigation:

- 5.1 users should upgrade to 5.1.1

- 5.0.x users should upgrade to 5.0.10
- 4.3.x users should upgrade to 4.3.20
- 4.2.x users should upgrade to a supported branch.

No further mitigation steps are necessary.

Note the following when evaluating the impact:

- Support for Range requests was introduced in version 4.2. Therefore versions prior to 4.2 are not affected by this issue.
- Support for returning an org.springfamework.core.io.Resource from an annotated controller was introduced in 5.0. Therefore versions prior to 5.0 can only be impacted through a registration to serve static resources.

https://pivotal.io/security/cve-2018-15756

Unify rates the priority as low to medium for our products.

Affected Products

Circuit Provisioning Agent is affected, fix version is 0.9.18

Circuit Backend Services / Operations Node is affected with low priority, fix is in work. Operations node is not accessible from the internet.

OpenScape Backup and recovery services are not affected.

All other products do not use Spring Framework or not affected versions.

Recommended Actions

Starting with Circuit Provisioning Agent 0.9.18, Spring Framework is no longer affected.
Upgrade to this version.

References

https://pivotal.io/security/cve-2018-15756

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-15756

https://spring.io/blog/2018/10/16/spring-project-vulnerability-reports-published

Advisory: OBSO-1812-01, 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