Security Advisory Report - OBSO-2204-01

Spring Framework Remote Code Execution Vulnerability (Spring4Shell, CVE-2022-22965)

Release Date:	2022-04-04 15:49:41
Last Update:	2022-04-14 17:56:22

Summary

Spring Framework contains a flaw in the CachedIntrospectionResults class in spring-beans/src/main/java/org/springframework/beans/CachedIntrospectionResults.java related to insecure introspection when using request parameter binding. This may allow a remote attacker to invoke arbitrary Java class methods and execute arbitrary code.

This issue is reported to affect Spring MVC and Spring WebFlux applications using Spring Framework with JDK 9 or higher.

The severity is rated critical.

According to the current status of the investigation Atos Unify products are not affected by the vulnerability.

Details

- A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit.
- However, the nature of vulnerability is more general, and there may be other ways to exploit it.
- Requirements for the specific exploit: JDK9 or higher; Apache Tomcat as the Servlet container; Packaged as WAR; spring-webmvc or spring-webflux dependency; Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19 and older versions.
- Users of affected versions should apply the following remediation: 5.3.x users should upgrade to 5.3.18+, 5.2.x users should upgrade to 5.2.20+

- The vulnerability is rated critical with a CVSS3.1 score of 9.8
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Affected Products

Products confirmed not affected

Products that are using the Spring Framework

Circuit
Atos Unify OpenScape 4000 V8 and V10 Platform
Atos Unify Virtual Care Collaboration Service V1
Atos Unify OpenScape Common Management Platform V7 and V10
Atos Unify OpenScape Composer V2
Atos Unify OpenScape First GEMMA V3
Atos Unify OpenScape Deployment Service V7 and V10
Atos Unify OpenScape Contact Center V10,V11
Atos Unify OpenScape Fault Management V10, V11 and V12
Atos Unify OpenScape UC Application V9 and V10
Atos Unify OpenScape Backup & Recovery Services

Products that are not using the Spring Framework

Atos Unify OpenScape Business V3
Atos Unify OpenScape Enterpise Express V9 and V10
Atos Unify OpenScape Voice (simplex deployments) V9 an V10
Atos Unify OpenScape 4000 V8 and V10 Assistant
Atos Unify OpenScape 4000 V8 and V10 CSTA
Atos Unify OpenScape 4000 V8 and V10 Loadware
Atos Unify OpenScape Voice (duplex deployments) V9 an V10
Atos Unify OpenScape First Response ESRP V9
Atos Unify OpenScape First Response BCF V10
Atos Unify OpenScape First Response ESAPP V1
Atos Unify OpenScape First Response PSS V1
Atos Unify OpenScape First Response MSBF V2
Atos Unify OpenScape Alarm Response Professional V4 and V5
Atos Unify OpenScape Xpert Clients V6 and V7
Atos Unify OpenScape Xpert MLC V6 and V7
Atos Unify OpenScape Xpert System Manager V6 and V7
Atos Unify OpenScape Branch V9 and V10
Atos Unify OpenScape SBC V9 and V10
Atos Unify OpenScape Contact Media Service V10,V11
Atos Unify OpenScape Fusion for Office V1 and V2
Atos Unify OpenScape Extensions for MS Outlook V1 and V2
Atos Unify OpenScape Fusion for Notes V1 and V2
Atos Unify OpenScape Web Collaboration V7
Atos Unify OpenScape Concierge V4
Atos Unify OpenScape Xpressions V7
Atos Unify OpenScape Personal Edition V7

Atos Unify OpenScape Media Server V9
Atos Unify OpenScape 4000 Manager V8 and V10
Atos Unify OpenScape Accounting Management V3, V4 and V5
Atos Unify OpenScape Voice Trace Manager V8
Atos Unify OpenScape Desk Phones CP SIP
Atos Unify OpenScape Desk Phones CP HFA
Atos Unify OpenScape Desk Phones IP SIP V3
Atos Unify OpenScape Desk Phones IP HFA V3
OpenStage HFA V3
OpenStage SIP V3
AC Win SL V3
HiPath CAP V3.0
HiPath DS-Win V4
Atos Unify OpenScape Sesap V2
Atos Unify OpenScape Cordless IP V2
Atos Unify OpenScape DECT Phone S5 and SL5
Atos Unify OpenScape DECT Phone S6, R6 and SL6
Atos Unify OpenScape WLAN Phone WL3 and WL4
Atos Unify OpenScape WLAN Phone Wireless Service Gateway
Atos Unify OpenScape Voice Survival Authority

Recommended Actions

At the current state of the investigation no further actions for Atos Unify products are required.

References

External References

- https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- https://tanzu.vmware.com/security/cve-2022-22965
- https://www.springcloud.io/post/2022-03/spring-0day-vulnerability/#gsc.tab=0
- https://de.tenable.com/blog/spring4shell-faq-spring-framework-remote-code-execution-vulnerability
- https://www.riskbasedsecurity.com/2022/03/30/springshell-vulnerability/
- https://www.praetorian.com/blog/spring-core-jdk9-rce
- Zero-Day Vulnerability Discovered in Java Spring Framework (darkreading.com)
- https://unit42.paloaltonetworks.com/cve-2022-22965-springshell/
- https://www.bleepingcomputer.com/news/security/new-spring-java-framework-zero-day-allows-remote-code-execution/
- https://github.com/spring-projects/spring-framework/releases/tag/v5.2.20.RELEASE
- https://github.com/spring-projects/spring-framework/releases/tag/v5.3.18

Change History

Version	Date	Description
1.0	04.04.2022	- Initial release
1.1	04.04.2022	- Atos Unify OpenScape Cordless IP V2 (not affected) - Atos Unify OpenScape DECT Phone S5 and SL5 (not affected) - Atos Unify OpenScape DECT Phone S6, R6 and SL6 (not affected)
1.2	07.04.2022	- Atos Unify OpenScape WLAN Phone WL3 and WL4 (not affected) - Atos Unify OpenScape WLAN Phone Wireless Service Gateway (not affected) - Updated evaluation for Atos Unify OpenScape DLS (using Spring Framework but not affected)
1.3	11.04.2022	- Atos Unify OpenScape Voice Survival Authority (not affected) - Atos Unify OpenScape Contact Center V10,V11 is using the Spring Framework but not affected - Atos Unify OpenScape Fault Management V10, V11 and V12 is using the Spring Framework but not affected - Atos Unify OpenScape UC Application V9 and V10 is using the Spring Framework but not affected
1.4	14.04.2022	- Atos Unify OpenScape Backup & Recovery Services is using the Spring Framework but not affected

Advisory: OBSO-2204-01, status: general release
Security Advisories are released as part of Atos Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com