interact

IA-2023-01: Various Vulnerabilities on Open-Source Libraries for POE (1.7.2, 1.8.1, 1.9 and 1.9.1)

Publication Date: 27/02/2023

Last Update: 27/02/2023

Current Version: 1.0

Summary

POE Envision Manager component uses spring-web component and other open source components which are vulnerable to the following vulnerabilities:

- CVE-2022-46364: cfx-core-3.4.1 [CVS score 9.8 Critical]
- CVE-2022-22965: spring-beans[CVS score 9.8 Critical]
- CVE-2022-22980: Spring-Data-MongoDB-4.0.1 [CVS score 9.8 Critical]
- CVE-2020-10683: Dom4j-1.6.1[CVS score 9.8 Critical]
- CVE-2018-1273: : Spring-Data-Commons-1.8.2 [CVS score 9.8 Critical]
- CVE-2016-1000027: spring-web-4.3.20 [CVS score 9.8 Critical]

The POE system is developed to largely mitigate the major effects of these vulnerabilities, but we recommend to install the system in a network with limited exposure.

Affected Products and Systems

The following Systems and products are affected.

Affected Product	Remediation
Interact Office POE – Envision Manager (also known as Interact Office Wired) version 1.7.2, 1.8.1, 1.9 and 1.9.1	A new version of Envision Manager (EM) which will fix the vulnerabilities is not yet available. We will update this advisory once it is.

Details

Interact Office POE Envision Manager versions 1.7.2, 1.8.1, 1.9 and 1.9.1 are impacted by the vulnerabilities described.

CVE-2016-1000027:

Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the

vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

CVE-2022-22965:

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 the vulnerability is more general, and there may be other ways to exploit it.

CVE-2022-22980:

A Spring Data MongoDB application is vulnerable to SpEL Injection when using @Query or @Aggregation-annotated query methods with SpEL expressions that contain query parameter placeholders for value binding if the input is not sanitized.

In the case of POE, the database access shall be limited to the application and therefore there is no actual impact.

CVE-2020-10683:

dom4j before 2.0.3 and 2.1.x before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.

CVE-2022-46364:

A SSRF vulnerability in parsing the href attribute of XOP:Include in MTOM requests in versions of Apache CXF before 3.5.5 and 3.4.10 allows an attacker to perform SSRF style attacks on webservices that take at least one parameter of any type.

CVE-2018-1273:

Spring Data Commons, versions prior to 1.13 to 1.13.10, 2.0 to 2.0.5, and older unsupported versions, contain a property binder vulnerability caused by improper neutralization of special elements. An unauthenticated remote malicious user (or attacker) can supply specially crafted request parameters against Spring Data REST backed HTTP resources or using Spring Data's projection-based request payload binding hat can lead to a remote code execution attack

Workaround and Mitigations

As a mitigation, please install EM in a secure network with limited exposure to the internet. Block all ports for the product going out to hosts that are not whitelisted.

General Security Recommendations

Vulnerability Classification

CVSS 3.x Severity and Metrics:

CVE-2022-46364: cfx-core-3.4.1 [CVS score 9.8 Critical]
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2022-22965: spring-beans[CVS score 9.8 Critical]
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2022-22980: Spring-Data-MongoDB-4.0.1 [CVS score 9.8 Critical]
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2020-10683: Dom4j-1.6.1[CVS score 9.8 Critical]
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2018-1273: : Spring-Data-Commons-1.8.2 [CVS score 9.8 Critical]
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2016-1000027: spring-web-4.3.20 [CVS score 9.8 Critical]
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Acknowledgements

Additional Information

Terms of Use

Signify Security Advisories are subject to the terms and conditions contained in Signify underlying license terms or other applicable agreements previously agreed to with Signify (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Signify Security Advisory, the Terms of Use of Signify Global Website: https://www.signify.com/global/conditions-of-commercial-sale . In case of conflicts, the License Terms shall prevail over the Terms of Use.