Vulnerabilities report: Vulnerabilities

Fri Aug 25, 2023

Created by: abaer1234@gmail.com

Produced at: Friday, 25-Aug-23 07:32:32 UTC

Severity	Issue	CVEs	Vulnerable component	Summary	Impacted Artifact	Repo Path	Published	Fix version	Project Key
Critical (Source: CVSS V3 from NVD)	XRAY-262821	CVE-2022-1471 CVSS3: 9.8	gav://org.yaml:snakeyaml:1.33	SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization.	gav://org.springframework.samples:spring-petclinic:3.1.0-SNAPSHOT	spj-libs-snapshot-local/org/springframework/samples/spring-petclinic/3.1.0-SNAPSHOT/spring-petclinic-3.1.0-20230825.064500-1.jar	2022-12-04	2.0	
Critical (Source: CVSS V3 from NVD)	XRAY-262821	CVE-2022-1471 CVSS3: 9.8	gav://org.yaml:snakeyaml:1.33	SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization.	gav://org.springframework.samples:spring-petclinic:3.1.0-SNAPSHOT	spj-libs-snapshot-local/org/springframework/samples/spring-petclinic/3.1.0-SNAPSHOT/spring-petclinic-3.1.0-20230825.065839-2.jar	2022-12-04	2.0	
High (Source: NVD)	XRAY-261922	CVE-2022-45868 CVSS3: 7.8	gav://com.h2database:h2:2.1.214	** DISPUTED ** The web-based admin console in H2 Database Engine through 2.1.214 can be started via the CLI with the argument -webAdminPassword, which allows the user to specify the password in cleartext for the web admin console. Consequently, a local user (or an attacker that has obtained local access through some means) would be able to discover the password by listing processes and their arguments. NOTE: the vendor states "This is not a vulnerability of H2 Console ... Passwords should never be passed on the command line and every qualified DBA or system administrator is expected to know that."	gav://org.springframework.samples:spring-petclinic:3.1.0-SNAPSHOT	spj-libs-snapshot-local/org/springframework/samples/spring-petclinic/3.1.0-SNAPSHOT/spring-petclinic-3.1.0-20230825.064500-1.jar	2022-11-24	2.2.220	

Severity	Issue	CVEs	Vulnerable component	Summary	Impacted Artifact	Repo Path	Published	Fix version	Project Key
High (Source: NVD)	XRAY-261922	CVE-2022-45868 CVSS3: 7.8	gav://com.h2database:h2:2.1.214	** DISPUTED ** The web-based admin console in H2 Database Engine through 2.1.214 can be started via the CLI with the argument -webAdminPassword, which allows the user to specify the password in cleartext for the web admin console. Consequently, a local user (or an attacker that has obtained local access through some means) would be able to discover the password by listing processes and their arguments. NOTE: the vendor states "This is not a vulnerability of H2 Console ... Passwords should never be passed on the command line and every qualified DBA or system administrator is expected to know that."	gav://org.springframework.samples:spring-petclinic:3.1.0-SNAPSHOT	spj-libs-snapshot-local/org/springframework/samples/spring-petclinic/3.1.0-SNAPSHOT/spring-petclinic-3.1.0-20230825.065839-2.jar	2022-11-24	2.2.220	
Medium (Source: CVSS V3 from NVD)	XRAY-522015	CVE-2023-35116 CVSS3: 4.7	gav://com.fasterxml.jackson.core:jackson-databind:2.15.2	An issue was discovered jackson-databind thru 2.15.2 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	gav://org.springframework.samples:spring-petclinic:3.1.0-SNAPSHOT	spj-libs-snapshot-local/org/springframework/samples/spring-petclinic/3.1.0-SNAPSHOT/spring-petclinic-3.1.0-20230825.064500-1.jar	2023-06-15		
Medium (Source: CVSS V3 from NVD)	XRAY-522015	CVE-2023-35116 CVSS3: 4.7	gav://com.fasterxml.jackson.core:jackson-databind:2.15.2	An issue was discovered jackson-databind thru 2.15.2 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	gav://org.springframework.samples:spring-petclinic:3.1.0-SNAPSHOT	spj-libs-snapshot-local/org/springframework/samples/spring-petclinic/3.1.0-SNAPSHOT/spring-petclinic-3.1.0-20230825.065839-2.jar	2023-06-15		