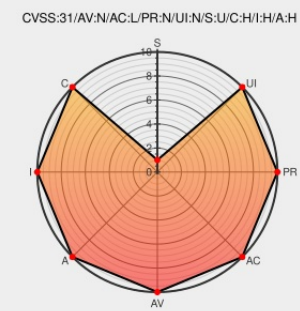
CVE-2022-22980

Published on: Not Yet Published

Last Modified on: 06/30/2022 07:13:00 PM UTC

CVE-2022-22980

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Spring Data Mongodb from Vmware contain the following vulnerability:

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.

CVE-2022-22980 has been assigned by security@vmware.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2022-22980 | Security | VMware Tanzu	tanzu.vmware.com text/html	MISC tanzu.vmware.com/security/cve-2022-22980

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

376684 Spring Data MongoDB SpEL Expression Injection Vulnerability

Exploit/POC from Github

CVE-2022-22980 exp demo可作为扫描器靶场

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Spring Data Mongodb	3.4.0	All	All	All
Application	Vmware	Spring Data Mongodb	All	All	All	All

cpe:2.3:a:vmware:spring_data_mongodb:3.4.0:*:*:*:*:*:*:*

cpe:2.3:a:vmware:spring_data_mongodb:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@SpringData	CVE report published for Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980). Please upgr… twitter.com/i/web/status/1…	2022-06-20 12:42:28
@RichardLaksana	Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980) ift.tt/rSKGTAV	2022-06-20 13:26:54
@NeriJimz	Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980) dlvr.it/SSXKtS	2022-06-20 20:32:32
@bbossola	@MeterianHQ tanzu.vmware.com/security/cve-2…	2022-06-20 23:14:44
@threedr3am1	[CVE-2022-22980] Spring Data MongoDB SpEL Expression injection vulnerability Learnning Demo. github.com/threedr3am/lea…	2022-06-21 12:37:30
@autumn_good_35	CVE-2022-22980: Spring Data MongoDB SpEL Expression injection vulnerability through annotated repository query meth… twitter.com/i/web/status/1…	2022-06-21 12:51:37
@momika233	github.com/kuron3k0/Sprin… CVE-2022-22980: Spring Data MongoDB SpEL Expression injection vulnerability through annotat… twitter.com/i/web/status/1…	2022-06-21 13:30:30
@piedpiper1616	GitHub - trganda/CVE-2022-22980: Poc of CVE-2022-22980 - github.com/trganda/CVE-20…	2022-06-21 15:56:09
@motikan2010	"CVE-2022-22980"が面白そう...。 PoCもチラホラ。だが寝る(˘ω˘)。 ーーー CVE-2022-22980 | Security | VMware Tanzu tanzu.vmware.com/security/cve-2… https://t.co/jY2gdU7vMw	2022-06-21 16:05:07
@ipssignatures	The vuln CVE-2022-22980 has a tweet created 0 days ago and retweeted 10 times. twitter.com/momika233/stat… #pow1rtrtwwcve	2022-06-21 16:06:00

@KasuyaMotu	にゃーん: CVE-2022-22980: Spring Data MongoDB SpEL Expression Injection vulnerability through annotated repository quer… twitter.com/i/web/status/1…	2022-06-21 16:19:55
@hack_git	CVE-2022-22980 Spring-Data-Mongodb-Example github.com/kuron3k0/Sprin… Research:tanzu.vmware.com/security/cve-2… #cve… twitter.com/i/web/status/1…	2022-06-21 20:10:43
@n0ipr0cs	CVE-2022-22980 | Security | VMware Tanzu tanzu.vmware.com/security/cve-2…	2022-06-21 23:08:47
@ipssignatures	The vuln CVE-2022-22980 has a tweet created 0 days ago and retweeted 14 times. twitter.com/threedr3am1/st… #pow1rtrtwwcve	2022-06-22 00:06:00
@secuner	New Vulnerability New vulnerability in Spring data MongoDB Library CVE-2022-22980 Affected products: Spring Dat… twitter.com/i/web/status/1…	2022-06-22 06:56:19
@Qianlingshan	Spring Data MongoDB SpEL表达式注入漏洞(CVE-2022-22980) #CVE #Spring #SpEL https://t.co/QUVGUlYgYp	2022-06-22 09:47:49
@hack_git	CVE-2022-22980 A local based poc of CVE-2022-22980 github.com/trganda/CVE-20… Research:tanzu.vmware.com/security/cve-2…… twitter.com/i/web/status/1…	2022-06-22 15:10:33
@ptracesecurity	Poc of CVE-2022-22980 github.com/trganda/CVE-20… #Pentesting #CVE #CyberSecurity #Infosec https://t.co/xGc9GmVhKO	2022-06-23 00:00:55
@sploitus_com	Exploit for CVE-2022-22980 sploitus.com/exploit?id=A03… #Exploit #Sploitus	2022-06-23 00:26:47
@cybersecboardrm	trganda/CVE-2022-22980: Poc of CVE-2022-22980 #Cybersecurity #infosec #security github.com/trganda/CVE-20…	2022-06-23 03:36:19
@Necio_news	trganda/CVE-2022-22980: Poc of CVE-2022-22980 #Infosec #cybersecurity #security github.com/trganda/CVE-20…	2022-06-23 04:18:19
@buaqbot	Update on Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980) ift.tt/dOAVjtg ift.tt/3FUvYn5	2022-06-23 07:24:07
@cornichecorp	trganda/CVE-2022-22980: Poc of CVE-2022-22980 #Cybersecurity #infosec #security via twinybots.ch github.com/trganda/CVE-20…	2022-06-23 07:44:15
@MnkeniFrancis	trganda/CVE-2022-22980: Poc of CVE-2022-22980 #Cybersecurity #infosec #security via twinybots.ch github.com/trganda/CVE-20…	2022-06-23 07:50:10
@cipherstorm	Update on Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980): Background On June 20, 2022… twitter.com/i/web/status/1…	2022-06-23 07:57:09
@corizance	trganda/CVE-2022-22980: Poc of CVE-2022-22980 #Cybersecurity #infosec #security via twinybots.ch github.com/trganda/CVE-20…	2022-06-23 08:03:31
@security_inside	Update on Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980) securityboulevard.com/2022/06/update…	2022-06-23 08:04:17
@csirt_it	Rilevato un #PoC per lo sfruttamento della CVE-2022-22980 relativa a Spring Data MongoDB Rischio: ? Tipologia: Re… twitter.com/i/web/status/1…	2022-06-23 08:05:53
@nicolaferrini	PoC pubblico per lo sfruttamento della CVE-2022-22980 (AL02/220623/CSIRT-ITA) csirt.gov.it/contenuti/poc-…	2022-06-23 08:29:33
@pocpeer	trganda/CVE-2022-22980: Poc1 of CVE-2022-22980 github.com/trganda/CVE-20…	2022-06-23 08:32:24
@the_yellow_fall	CVE-2022-22980: Spring Data MongoDB SpEL Expression injection vulnerability securityonline.info/cve-2022-22980… #opensource… twitter.com/i/web/status/1…	2022-06-23 09:11:20
@SinetNews	PoC pubblico per lo sfruttamento della CVE-2022-22980 (AL02/220623/CSIRT-ITA) ift.tt/8aXAPjf	2022-06-23 09:14:23
@AcooEdi	CVE-2022-22980: Spring Data MongoDB SpEL Expression injection vulnerability dlvr.it/SShbWK via securityonline	2022-06-23 09:17:12

@netsecu	securityboulevard.com/2022/06/update… Update on Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980) #cybersecurity	2022-06-23 09:46:05
@buaqbot	Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980) POC ift.tt/OqkPdNh ift.tt/yHDalim	2022-06-23 10:06:33
@infosec_intel	github.com/trganda/CVE-20… #infosec #redteam #pentesting #hackingtools #cybersecurity	2022-06-23 12:06:41
@CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2022-30190: 986.1K (audience size) CVE-2022-22980: 269.3K CVE-2022… twitter.com/i/web/status/1…	2022-06-23 13:00:03
@Har_sia	CVE-2022-22980 har-sia.info/CVE-2022-22980… #HarsiaInfo	2022-06-23 15:00:07
@d0znpp	Did you hear about #Mongo4shell / CVE-2022-22980 already? This is the next SpEL exploit in a row. lnkd.in/gBtyqzj3	2022-06-23 16:17:13
@CVEreport	CVE-2022-22980 : A Spring Data MongoDB application is vulnerable to SpEL Injection when using @Query or… twitter.com/i/web/status/1…	2022-06-23 16:52:18
@0xbadad	trganda/CVE-2022-22980: Poc of CVE-2022-22980 #Cybersecurity #infosec #security via twinybots.ch github.com/trganda/CVE-20…	2022-06-23 18:51:59
@LinInfoSec	Mongodb - CVE-2022-22980: tanzu.vmware.com/security/cve-2…	2022-06-23 19:00:05
@d0znpp	Did you hear about mongo4shell SpEL exploit for @mongodb? lab.wallarm.com/update-on-spri… #rce #owasp #mongodb	2022-06-23 21:54:34
/r/InfoSecWriteups	Analyzing CVE-2022–22980 to discover a real exploitable path in the source code review process with…	2022-06-27 15:50:56
/r/worldTechnology	Update on Spring Data MongoDB SpEL Expression Injection Vulnerability (CVE-2022-22980)	2022-06-30 23:17:28
/r/cybersecurity	why did spring data vulns become the hot vuln for a bit?	2022-07-06 02:13:54

← Previous ID

Next ID→