



CVE-2022-31679

Published on: Not Yet Published

Last Modified on: 09/22/2022 07:42:00 PM UTC

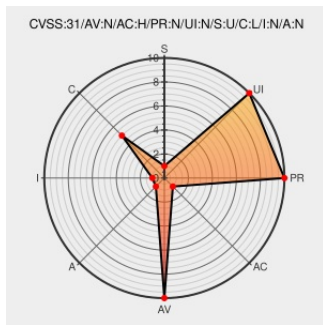
CVE-2022-31679

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Spring Data Rest](#) from [Vmware](#) contain the following vulnerability:

Applications that allow HTTP PATCH access to resources exposed by Spring Data REST in versions 3.6.0 - 3.5.5, 3.7.0 - 3.7.2, and older unsupported versions, if an attacker knows about the structure of the underlying domain model, they can craft HTTP requests that expose hidden entity attributes.

CVE-2022-31679 has been assigned by [vmw](#) security@vmware.com to track the vulnerability - currently rated as **LOW** severity.

CVSS3 Score: **3.7 - LOW**

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

CVE References

Description	Tags	Link
CVE-2022-31679 Security VMware Tanzu	tanzu.vmware.com text/html	vmw MISC tanzu.vmware.com/security/cve-2022-31679

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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.









There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	VMware	Spring Data Rest	All	All	All	All
cpe:2.3:a:vmware:spring_data_rest:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @springcentral	new from @odrotbohm: Spring Data REST Vulnerability (CVE-2022-31679) #springboot spring.io/blog/2022/09/1...	2022-09-19 16:06:16
 @RichardLaksana	Spring Data REST Vulnerability (CVE-2022-31679) ift.tt/02hvG97	2022-09-19 16:26:54
 @odrotbohm	@Bedzon @springcentral Details are here (also linked to from the blog post): tanzu.vmware.com/security/cve-2...	2022-09-19 16:48:37
 @NeriJimz	Spring Data REST Vulnerability (CVE-2022-31679) dldr.it/SYcrpM https://t.co/6HWTuyv9Bv	2022-09-19 20:32:36
 @CVEreport	CVE-2022-31679 : Applications that allow HTTP PATCH access to resources exposed by Spring Data REST in versions 3.6... twitter.com/i/web/status/1...	2022-09-21 18:05:25
 @LinInfoSec	Spring - CVE-2022-31679: tanzu.vmware.com/security/cve-2...	2022-09-21 21:00:33
 /r/netcve	CVE-2022-31679	2022-09-21 19:39:12
 /r/websecurityresearch	CVE-2022-31679: Potential Unintended Data Exposure for Resource Exposed by Spring Data REST - Applications that allow HTTP PATCH access to resources exposed by Spring Data REST, if an attacker knows about the underlying domain model, they can craft requests that expose hidden entity attributes	2022-09-22 06:07:48

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report