



CVE-2022-31692

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2022-31692
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-31 20:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	Spring Security, versions 5.7 prior to 5.7.5 and 5.6 prior to 5.6.9 could be susceptible to authorization rules bypass via forw...

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Vmware	Spring Security	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2022-31692 Security VMware Tanzu	MISC	tanzu.vmware.com	
October 2022 Spring Security Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[241340](#) Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:1655)

[770184](#) Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:1655)

© [CVE.report](#) 2026 |

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](#)