



CVE-2021-22119

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

Summary

CVE	CVE-2021-22119
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-29 17:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	Spring Security versions 5.5.x prior to 5.5.1, 5.4.x prior to 5.4.7, 5.3.x prior to 5.3.10 and 5.2.x prior to 5.2.11 are susceptible

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Communications Cloud Native Core Policy	1.14.0	All	All	All
Application	Vmware	Spring Security	All	All	All	All

References

Reference
Pony Mail!
[portals-pluto-dev] 20210714 [jira] [Updated] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-
Pony Mail!
[portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-786 Upgrade to version Spring Framework 5.3.7 and Spring Sec
[portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2
Pony Mail!
Pony Mail!
[portals-pluto-dev] 20210714 [jira] [Reopened] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CV
Oracle Critical Patch Update Advisory - January 2022
[nifi-issues] 20210726 [jira] [Created] (NIFI-8948) Upgrade Spring Framework to 5.3.9 and Spring Security to 5.5.1
Pony Mail!
Pony Mail!

CVE-2021-22119: Denial-of-Service (DoS) attack via initiation of Authorization Request in Spring Security OAuth 2.0 Client Web and WebFlux

[portals-pluto-dev] 20210714 [jira] [Comment Edited] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due

Oracle Critical Patch Update Advisory - July 2022

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981979](#) Java (maven) Security Update for org.springframework.security:spring-security-oauth2-client (GHSA-w9jg-gvgr-354m)

© [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](#)