



CVE-2020-5407

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-5407
State	PUBLIC
Assigner	security@pivotal.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-13 17:15:00 UTC
Updated	2023-11-07 03:23:00 UTC
Description	Spring Security versions 5.2.x prior to 5.2.4 and 5.3.x prior to 5.3.2 contain a signature wrapping vulnerability during SAML

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal Software	Spring Security	All	All	All	All
Application	Pivotal Software	Spring Security	All	All	All	All

References

Reference	Source	Link
Pony Mail!		lists.
Pony Mail!		lists.
Pony Mail!	MLIST	lists.
Oracle Critical Patch Update Advisory - October 2020	MISC	www
Pony Mail!		lists.
CVE-2020-5407: Signature Wrapping Vulnerability with spring-security-saml2-service-provider Security VMware Tanzu	CONFIRM	tanz
Pony Mail!	MLIST	lists.
Pony Mail!	MLIST	lists.
Oracle Critical Patch Update Advisory - April 2021	MISC	www
Oracle Critical Patch Update Advisory - January 2021	MISC	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982251](#) Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-48rw-j489-928m)

© [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](#)