Unauthorized User Impersonation when Using X.509 Client Certificates

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-22747
State	PUBLISHED
Assigner	vmware
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 06:16:03 UTC
Updated	2026-04-22 06:16:03 UTC
Description	Vulnerability in Spring Spring Security. SubjectX500PrincipalExtractor does not correctly handle certain malformed X.509 ce

Risk And Classification

Primary CVSS: v3.1 6.8 MEDIUM from security@vmware.com

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N

Version	Source	Type	Score	Severity	Vector
3.1	security@vmware.com	Secondary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
High

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Spring	Spring Security	affected 7.0.0 7.0.4 custom	Not specified

References

Reference	Source	Link	Tags
spring.io/security/cve-2026-22747	security@vmware.com	spring.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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 registred 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.

Free CVE JSON API cve.report/api

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