



Stored Cross-Site Scripting (XSS) Vulnerability

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

Summary

CVE	CVE-2026-3007
State	PUBLISHED
Assigner	CSA
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 04:16:07 UTC
Updated	2026-04-23 04:16:07 UTC
Description	Successful exploitation of the stored cross-site scripting (XSS) vulnerability could allow an attacker to execute arbitrary Java

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from 5f57b9bf-260d-4433-bf07-b6a79e9bb7d4

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

Version	Source	Type	Score	Severity	Vector
3.1	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Three Learning	Koollab Learning Management System	affected 5.3.2.	Not specified

References

Reference	Source	Link	Tags
www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-042	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	www.csa.gov.sg	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Justin Ng (en)

Additional Advisory Data

Solutions

CNA: Users and administrators of the affected product version are advised to update to the latest version 5.4.0 immediately.

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 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](#).

Free CVE JSON API cve.report/api

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