



CVE-2026-40212

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

Summary

CVE	CVE-2026-40212
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 08:16:25 UTC
Updated	2026-04-10 16:16:32 UTC
Description	OpenStack Skyline before 5.0.1, 6.0.0, and 7.0.0 has a DOM-based Cross-Site Scripting (XSS) vulnerability in the console

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from cve@mitre.org

[CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N](#)

EPSS: 0.000300000 probability, percentile 0.086920000 (date 2026-04-11)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	cve@mitre.org	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

ntegrity

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	OpenStack	Skyline	affected 5.0.1 semver	Not specified
CNA	OpenStack	Skyline	affected 6.0.0 semver	Not specified
CNA	OpenStack	Skyline	affected 7.0.0 semver	Not specified

References

Reference	Source	Link	Tags
bugs.launchpad.net/skyline-console/+bug/2138575	cve@mitre.org	bugs.launchpad.net	
www.openwall.com/lists/oss-security/2026/04/09/30	cve@mitre.org	www.openwall.com	
security.openstack.org/ossa/OSSA-2026-006.html	cve@mitre.org	security.openstack.org	
review.opendev.org/973351	cve@mitre.org	review.opendev.org	
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 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