



SolarWinds Observability Self-Hosted Stored Cross-Site Scripting Vulnerability

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

Summary

CVE	CVE-2026-28297
State	PUBLISHED
Assigner	SolarWinds
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 15:16:34 UTC
Updated	2026-03-31 14:14:02 UTC
Description	SolarWinds Observability Self-Hosted was found to be affected by a stored cross-site scripting vulnerability, which when ex

Risk And Classification

Primary CVSS: v3.1 8.7 HIGH from nvd@nist.gov

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

EPSS: 0.000720000 probability, percentile 0.220360000 (date 2026-04-02)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.7	HIGH	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
3.1	psirt@solarwinds.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	Observability Self-hosted	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SolarWinds	SolarWinds Observability Self-Hosted	affected 2026.1.1 and previous versions	Windows

References

Reference	Source	Link
documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/hco_202...	psirt@solarwinds.com	documentation.s
www.solarwinds.com/trust-center/security-advisories/CVE-2026-28297	psirt@solarwinds.com	www.solarwinds
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Steven Karschnia - Armadin (en)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)