



# Handlebars.js has JavaScript Injection in CLI Precompiler via Unescaped Names and Options

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

## Summary

<b>CVE</b>	CVE-2026-33941
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-27 22:16:21 UTC
<b>Updated</b>	2026-03-31 17:53:18 UTC
<b>Description</b>	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, the Handlebars CLI precompiler has a JavaScript injection vulnerability via unescaped names and options.

## Risk And Classification

**Primary CVSS:** v3.1 8.2 HIGH from nvd@nist.gov

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

**EPSS:** 0.000180000 probability, percentile 0.047150000 (date 2026-04-01)

**Problem Types:** CWE-79 | CWE-94 | CWE-116 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection') | CWE-116 CWE-116: Improper Encoding or Escaping of Output

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	8.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Handlebarsjs</a>	<a href="#">Handlebars</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Handlebars-lang</a>	<a href="#">Handlebars.js</a>	affected >= 4.0.0, < 4.7.9	Not specified

### References

Reference	Source	Link	Tags
<a href="#">github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-xjpx-3...</a>	security-advisories@github.com	<a href="#">github.com</a>	Exploit,
<a href="#">github.com/handlebars-lang/handlebars.js/releases/tag/v4.7.9</a>	security-advisories@github.com	<a href="#">github.com</a>	Release
<a href="#">github.com/handlebars-lang/handlebars.js/commit/68d8df5a88e0a26fe9e6084c...</a>	security-advisories@github.com	<a href="#">github.com</a>	Patch
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonic

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](#).

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