



CVE-2013-4170

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2013-4170
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-30 13:15:00 UTC
Updated	2022-07-09 02:07:00 UTC
Description	In general, Ember.js escapes or strips any user-supplied content before inserting it in strings that will be sent to innerHTML.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emberjs	Ember.js	All	All	All	All
Application	Emberjs	Ember.js	1.0.0	rc1	All	All
Application	Emberjs	Ember.js	1.0.0	rc2	All	All
Application	Emberjs	Ember.js	1.0.0	rc3	All	All
Application	Emberjs	Ember.js	1.0.0	rc4	All	All
Application	Emberjs	Ember.js	1.0.0	rc5	All	All
Application	Emberjs	Ember.js	1.0.0	rc6	All	All

References

Reference	Source	L
CVE-2013-4170 (ember-source): Ember.js Potential XSS Exploit When Binding `tagName` to User-Supplied Data - RubySec	MISC	r
[CVE-2013-4170] Potential XSS Exploit When Binding `tagName` to User-Supplied Data	MISC	g
Cross-site Scripting (XSS) in ember-source CVE-2013-4170 Snyk	MISC	s
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	n

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](#)