



CVE-2018-14041

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

Summary

CVE	CVE-2018-14041
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-13 14:29:00 UTC
Updated	2023-11-07 02:52:00 UTC
Description	In Bootstrap before 4.1.2, XSS is possible in the data-target property of scrollspy.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Getbootstrap	Bootstrap	All	All	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha2	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha3	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha4	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha5	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha6	All	All
Application	Getbootstrap	Bootstrap	4.0.0	beta	All	All
Application	Getbootstrap	Bootstrap	4.0.0	beta2	All	All
Application	Getbootstrap	Bootstrap	4.0.0	beta3	All	All
Application	Getbootstrap	Bootstrap	All	All	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha2	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha3	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha4	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha5	All	All
Application	Getbootstrap	Bootstrap	4.0.0	alpha6	All	All

Application	Getbootstrap	Bootstrap	4.0.0	beta	All	All
Application	Getbootstrap	Bootstrap	4.0.0	beta2	All	All
Application	Getbootstrap	Bootstrap	4.0.0	beta3	All	All

References

Reference	Source	Link
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
XSS possible in data-target property of scrollspy · Issue #26627 · twbs/bootstrap · GitHub	MISC	github.com
dotCMS 5.1.1 Vulnerable Dependencies ~ Packet Storm	MISC	packetstormsec.com
Pony Mail!	MLIST	lists.apache.org
Fix xss in tooltip, collapse and scrollspy plugins by Johann-S · Pull Request #26630 · twbs/bootstrap · GitHub	MISC	github.com
v4.1.2 ship list · Issue #26423 · twbs/bootstrap · GitHub	MISC	github.com
Full Disclosure: dotCMS v5.1.1 HTML Injection & XSS Vulnerability	FULLDISC	seclists.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
OctoberCMS Insecure Dependencies ~ Packet Storm	MISC	packetstormsec.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Full Disclosure: dotCMS v5.1.1 Vulnerabilities	FULLDISC	seclists.org
Full Disclosure: Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability	FULLDISC	seclists.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Bugtraq: dotCMS v5.1.1 Vulnerabilities	BUGTRAQ	seclists.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com
Pony Mail!		lists.apache.org
Bootstrap 4.1.2 · Bootstrap Blog	MISC	blog.getbootstrap.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[241153](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0554)

[241154](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0550)

[241154](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0552)

[241155](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0553)

[982265](#) Nodejs (npm) Security Update for bootstrap (GHSA-pj7m-g53m-7638)

© [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](#)