



# CVE-2018-14042

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2018-14042  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2018-07-13 14:29:00 UTC   |
| <b>Updated</b>         | 2023-11-07 02:52:00 UTC   |
| <b>Description</b>     | In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip. |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                       | Product                   | Version | Update | Edition | Language |
|-------------|------------------------------|---------------------------|---------|--------|---------|----------|
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | All     | All    | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha  | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha2 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha3 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha4 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha5 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha6 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | beta   | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | beta2  | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | beta3  | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | All     | All    | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha  | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha2 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha3 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha4 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha5 | All     | All      |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0   | alpha6 | All     | All      |

|             |                              |                           |       |       |     |     |
|-------------|------------------------------|---------------------------|-------|-------|-----|-----|
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0 | beta  | All | All |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0 | beta2 | All | All |
| Application | <a href="#">Getbootstrap</a> | <a href="#">Bootstrap</a> | 4.0.0 | beta3 | All | All |

## References

| Reference  | Source   | Link  |
|--|----------|---|
| Pony Mail!   |          | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Pony Mail!   |          | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Pony Mail!   | MLIST    | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Pony Mail!   |          | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Fix xss in tooltip, collapse and scrollspy plugins by Johann-S · Pull Request #26630 · twbs/bootstrap · GitHub | MISC     | <a href="https://github.com">github.com</a>                       |
| Pony Mail!   | MLIST    | <a href="https://lists.apache.org">lists.apache.org</a>           |
| v4.1.2 ship list · Issue #26423 · twbs/bootstrap · GitHub  | MISC     | <a href="https://github.com">github.com</a>                       |
| XSS possible in data-container property of tooltip · Issue #26628 · twbs/bootstrap · GitHub                    | MISC     | <a href="https://github.com">github.com</a>                       |
| Full Disclosure: dotCMS v5.1.1 HTML Injection & XSS Vulnerability  | FULLDISC | <a href="https://seclists.org">seclists.org</a>                   |
| [R1] Tenable.sc 5.19.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory   Tenable®               | CONFIRM  | <a href="https://www.tenable.com">www.tenable.com</a>             |
| Pony Mail!   | MLIST    | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Pony Mail!   |          | <a href="https://lists.apache.org">lists.apache.org</a>           |
| OctoberCMS Insecure Dependencies ≈ Packet Storm  | MISC     | <a href="https://packetstormsec.com">packetstormsec.com</a>       |
| Pony Mail!   |          | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Pony Mail!   | MLIST    | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Full Disclosure: dotCMS v5.1.1 Vulnerabilities   | FULLDISC | <a href="https://seclists.org">seclists.org</a>                   |
| Full Disclosure: Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability  | FULLDISC | <a href="https://seclists.org">seclists.org</a>                   |
| Bugtraq: dotCMS v5.1.1 Vulnerabilities   | BUGTRAQ  | <a href="https://seclists.org">seclists.org</a>                   |
| Pony Mail!   | MLIST    | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Pony Mail!   | MLIST    | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Oracle Critical Patch Update Advisory - April 2021   | MISC     | <a href="https://www.oracle.com">www.oracle.com</a>               |
| Pony Mail!   |          | <a href="https://lists.apache.org">lists.apache.org</a>           |
| Bootstrap 4.1.2 · Bootstrap Blog   | MISC     | <a href="https://blog.getbootstrap.com">blog.getbootstrap.com</a> |
| CVE Program record   | CVE.ORG  | <a href="https://www.cve.org">www.cve.org</a>                     |
| NVD vulnerability detail   | NVD      | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159652 Oracle Enterprise Linux Security Update for idm:d1 and idm:client (ELSA-2020-4670)

|   |
|---|
| <a href="#">159679</a> Oracle Enterprise Linux Security Update for pki-core:10.6 and pki-deps:10.6 (ELSA-2020-4847)   |
| <a href="#">241153</a> Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0554)  |
| <a href="#">241154</a> Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0552)  |
| <a href="#">241155</a> Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0553)  |
| <a href="#">376093</a> F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Bootstrap Vulnerability (K19785240) |
| <a href="#">377492</a> Alibaba Cloud Linux Security Update for ipa (ALINUX2-SA-2020:0169)   |
| <a href="#">590764</a> Mitsubishi Electric EcoWebServerIII Multiple Vulnerabilities (ICSA-22-055-02)  |
| <a href="#">590808</a> Mitsubishi Electric EcoWebServerIII Multiple Vulnerabilities (ICSA-22-055-02)  |
| <a href="#">940071</a> AlmaLinux Security Update for idm:DL1 and idm:client (ALSA-2020:4670)  |
| <a href="#">940348</a> AlmaLinux Security Update for pki-core:10.6 and pki-deps:10.6 (ALSA-2020:4847)   |
| <a href="#">960340</a> Rocky Linux Security Update for idm:DL1 and idm:client (RLSA-2020:4670)  |
| <a href="#">960454</a> Rocky Linux Security Update for pki-core:10.6 and pki-deps:10.6 (RLSA-2020:4847)   |
| <a href="#">997450</a> NodeJs (Npm) Security Update for bootstrap (GHSA-7mvr-5x2g-wfc8)   |

© [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](#)**