Product Security Report for test

Generated: Mar 28, 2022

Findings

High

Finding 1: Hard Coded SSH Private Key Found in File

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	Active, Verified	March 27, 2022	1 days	(admin)	798 (https://cwe.mitre.org/data/definitions/798.html)	419

Location

File Path	Line Number
file	1

CVSS v3

None

Description

Secret: -----BEGIN OPENSSH PRIVATE KEY-----

Match: -----BEGIN OPENSSH PRIVATE KEY-----

Commit message: Add new file

Commit hash: 47e789035e7b2d0313a3ac59324cb5e6e44f93c2

Commit date: 2022-03-27T14:15:31Z

Rule Id: OPENSSH-PK

Secret: -----BEGIN OPENSSH PRIVATE KEY-----

Match: -----BEGIN OPENSSH PRIVATE KEY-----

Commit message: Add new file

Commit hash: 3ffba729c7c01cf0dc72929e7846ef9a6d1c2cb1

Commit date: 2022-03-27T14:32:03Z

Rule Id: OPENSSH-PK

Mitigation

None

Impact

None

Finding 2: Hard Coded Generic API Key Found in scripts/runSonarQube.sh

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	Active, Verified	March 27, 2022	1 days	(admin)	798 (https://cwe.mitre.org/data/definitions/798.html)	420

Location

File Path	Line Number
scripts/runSonarQube.sh	7

CVSS v3

None

Description

Secret: 291e50b66b5f5198e6ac0d49bf1057ac3a3a0fc8

Match: token="291e50b66b5f5198e6ac0d49bf1057ac3a3a0fc8"

Commit message: more preconditions checks

Commit hash: bf0cfdd19159c9a3852d589379583675c1b8a5a5

Commit date: 2021-09-18T20:39:18Z

Rule Id: generic-api-key

Mitigation

None

Impact

None

Medium

Finding 3: bootstrap:3.3.4 | CVE-2016-10735

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	421

Location

File Path	Line Number
bootstrap.js	None

CVSS v3

None

Description

In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:1456

Name: RHSA-2019:1456

Source: REDHAT

URL: https://access.redhat.com/errata/RHBA-2019:1076

Name: RHBA-2019:1076

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/27915#issuecomment-452140906

Source: REDHAT

URL: https://access.redhat.com/errata/RHBA-2019:1570

Name: RHBA-2019:1570

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26460

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/23687

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3023

Name: RHSA-2019:3023

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2020:0133

Name: RHSA-2020:0133

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2020:0132

Name: RHSA-2020:0132

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/20184

Source: info

URL: https://github.com/advisories/GHSA-4p24-vmcr-4gqj

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/23679

Source: MISC

URL: https://blog.getbootstrap.com/2018/12/13/bootstrap-3-4-0/

Finding 4: bootstrap:3.3.4 | CVE-2018-14040

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	422

Location

File Path	Line Number
bootstrap.js	None

CVSS v3

None

Description

In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL: https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL:
https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL:
https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26630

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26625

Source: info

URL: https://github.com/twbs/bootstrap/issues/20184

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26423

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL:
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: MISC

URL: https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/

Source: MLIST

URL: https://lists.debian.org/debian-lts-announce/2018/08/msg00027.html

Name: [debian-lts-announce] 20180827 [SECURITY] [DLA 1479-1] twitter-bootstrap3 security update

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26@%3Ccommits.pulsar.apache.org%3E

Name: [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list

Source: MISC

URL: http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html

Finding 5: bootstrap:3.3.4 | CVE-2018-14041

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	423

Location

File Path	Line Number
bootstrap.js	None

CVSS v3

None

Description

In Bootstrap before 4.1.2, XSS is possible in the data-target property of scrollspy.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL: https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:1456

Name: RHSA-2019:1456

Source: MLIST

URL: https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26630

Source: info

URL: https://github.com/twbs/bootstrap/issues/20184

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26423

Source: MLIST

URL: https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: MISC

URL: https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26627

Source: MISC

URL: http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html

Finding 6: bootstrap:3.3.4 | CVE-2018-14042

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	424

Location

File Path	Line Number
bootstrap.js	None

CVSS v3

None

Description

In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL: https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26630

Source: info

URL: https://github.com/twbs/bootstrap/issues/20184

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26423

Source: MLIST

URL: https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: MISC

URL: https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26628

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26@%3Ccom mits.pulsar.apache.org%3E

Name: [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list

Finding 7: bootstrap:3.3.4 | CVE-2019-8331

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	425

Location

File Path	Line Number
bootstrap.js	None

CVSS v3

None

Description

In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL: https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:1456

Name: RHSA-2019:1456

Source: CONFIRM

URL: https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/

Source: MLIST

URL:
https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MLIST

URL:
https://lists.apache.org/thread.html/54df3aeb4239b64b50b356f0ca6f986e3c4ca5b84c515dce077c7854@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190811 Apache flink 1.7.2 security issues

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MLIST

URL:
https://lists.apache.org/thread.html/17ff53f7999e74fbe3cc0ceb4e1c3b00b180b7c5afec8e978837bc49@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190813 Apache flink 1.7.2 security issues

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/52bafac05ad174000ea465fe275fd3cc7bd5c25535a7631c0bc9bfb2@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190813 Re: Apache flink 1.7.2 security issues

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26@%3Ccommits.pulsar.apache.org%3E

Name: [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list

Source: MLIST

URL: https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: info

URL: https://github.com/twbs/bootstrap/issues/28236

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/28236

Source: BID

URL: http://www.securityfocus.com/bid/107375

Name: 107375

Source: MLIST

URL:
https://lists.apache.org/thread.html/10f0f3aefd51444d1198c65f44ffdf2d78ca3359423dbc1c168c9731@%3Cdev.flink.apache.org%3E

Name: [flink-dev] 20190811 Apache flink 1.7.2 security issues

Source: CONFIRM

URL: https://support.f5.com/csp/article/K24383845?utm_source=f5support&utm_medium=RSS

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3023

Name: RHSA-2019:3023

Source: MLIST

URL:
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: CONFIRM

URL: https://support.f5.com/csp/article/K24383845

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: MISC

URL: https://github.com/twbs/bootstrap/releases/tag/v4.3.1

Source: MISC

URL: https://github.com/twbs/bootstrap/releases/tag/v3.4.1

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3024

Name: RHSA-2019:3024

Finding 8: bootstrap:3.3.4 | CVE-2016-10735

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	426

Location

File Path	Line Number
bootstrap.min.js	None

CVSS v3

None

Description

In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.min.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:1456

Name: RHSA-2019:1456

Source: REDHAT

URL: https://access.redhat.com/errata/RHBA-2019:1076

Name: RHBA-2019:1076

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/27915#issuecomment-452140906

Source: REDHAT

URL: https://access.redhat.com/errata/RHBA-2019:1570

Name: RHBA-2019:1570

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26460

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/23687

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3023

Name: RHSA-2019:3023

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2020:0133

Name: RHSA-2020:0133

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2020:0132

Name: RHSA-2020:0132

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/20184

Source: info

URL: https://github.com/advisories/GHSA-4p24-vmcr-4gqj

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/23679

Source: MISC

URL: https://blog.getbootstrap.com/2018/12/13/bootstrap-3-4-0/

Finding 9: bootstrap:3.3.4 | CVE-2018-14040

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	427

Location

File Path	Line Number
bootstrap.min.js	None

CVSS v3

None

Description

In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.min.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL:
https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL:
https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL:
https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26630

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26625

Source: info

URL: https://github.com/twbs/bootstrap/issues/20184

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26423

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL:
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: MISC

URL: https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/

Source: MLIST

URL: https://lists.debian.org/debian-lts-announce/2018/08/msg00027.html

Name: [debian-lts-announce] 20180827 [SECURITY] [DLA 1479-1] twitter-bootstrap3 security update

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26@%3Ccommits.pulsar.apache.org%3E

Name: [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list

Source: MISC

URL: http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html

Finding 10: bootstrap:3.3.4 | CVE-2018-14041

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	428

Location

File Path	Line Number
bootstrap.min.js	None

CVSS v3

None

Description

In Bootstrap before 4.1.2, XSS is possible in the data-target property of scrollspy.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.min.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL: https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:1456

Name: RHSA-2019:1456

Source: MLIST

URL: https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26630

Source: info

URL: https://github.com/twbs/bootstrap/issues/20184

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26423

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL:
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: MISC

URL: https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26627

Source: MISC

URL: http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html

Finding 11: bootstrap:3.3.4 | CVE-2018-14042

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	429

Location

File Path	Line Number
bootstrap.min.js	None

CVSS v3

None

Description

In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.min.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL: https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/26630

Source: info

URL: https://github.com/twbs/bootstrap/issues/20184

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26423

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL:
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: MISC

URL: https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: MISC

URL: https://github.com/twbs/bootstrap/issues/26628

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL:
https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26@%3Ccommits.pulsar.apache.org%3E

Name: [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list

Finding 12: bootstrap:3.3.4 | CVE-2019-8331

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	430

Location

File Path	Line Number
bootstrap.min.js	None

CVSS v3

None

Description

In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/scorecard/content/js/bootstrap.min.js

Mitigation

Update bootstrap:3.3.4 to at least the version recommended in the description

Impact

None

References

Source: MLIST

URL:
https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e@%3Cdev.superset.apache.org%3E

Name: [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:1456

Name: RHSA-2019:1456

Source: CONFIRM

URL: https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/

Source: MLIST

URL:
https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MLIST

URL:
https://lists.apache.org/thread.html/54df3aeb4239b64b50b356f0ca6f986e3c4ca5b84c515dce077c7854@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190811 Apache flink 1.7.2 security issues

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-14

Source: MLIST

URL:
https://lists.apache.org/thread.html/17ff53f7999e74fbe3cc0ceb4e1c3b00b180b7c5afec8e978837bc49@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190813 Apache flink 1.7.2 security issues

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/52bafac05ad174000ea465fe275fd3cc7bd5c25535a7631c0bc9bfb2@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190813 Re: Apache flink 1.7.2 security issues

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26@%3Ccommits.pulsar.apache.org%3E

Name: [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list

Source: MLIST

URL: https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714@%3Cissues.hbase.apache.org%3E

Name: [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: info

URL: https://github.com/twbs/bootstrap/issues/28236

Source: MISC

URL: https://github.com/twbs/bootstrap/pull/28236

Source: BID

URL: http://www.securityfocus.com/bid/107375

Name: 107375

Source: MLIST

URL:
https://lists.apache.org/thread.html/10f0f3aefd51444d1198c65f44ffdf2d78ca3359423dbc1c168c9731@%3Cdev.flink.apache.org%3E

Name: [flink-dev] 20190811 Apache flink 1.7.2 security issues

Source: CONFIRM

URL: https://support.f5.com/csp/article/K24383845?utm_source=f5support&utm_medium=RSS

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3023

Name: RHSA-2019:3023

Source: MLIST

URL:
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: CONFIRM

URL: https://support.f5.com/csp/article/K24383845

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: MISC

URL: https://github.com/twbs/bootstrap/releases/tag/v4.3.1

Source: MISC

URL: https://github.com/twbs/bootstrap/releases/tag/v3.4.1

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3024

Name: RHSA-2019:3024

Finding 13: jquery:2.1.4 | CVE-2015-9251

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	431

Location

File Path	Line Number
jquery.min.js	None

CVSS v3

None

Description

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/src/main/webapp/js/jquery.min.js

Mitigation

Update jquery:2.1.4 to at least the version recommended in the description

Impact

None

References

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuoct2020.html

Source: CONFIRM

URL: https://security.netapp.com/advisory/ntap-20210108-0004/

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: MLIST

URL: https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujul2020.html

Source: MLIST

URL: https://lists.apache.org/thread.html/54df3aeb4239b64b50b356f0ca6f986e3c4ca5b84c515dce077c7854@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190811 Apache flink 1.7.2 security issues

Source: MISC

URL: https://github.com/jquery/jquery/issues/2432

Source: MISC

URL: https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: MLIST

URL: https://lists.apache.org/thread.html/17ff53f7999e74fbe3cc0ceb4e1c3b00b180b7c5afec8e978837bc49@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190813 Apache flink 1.7.2 security issues

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2020-03/msg00041.html

Name: openSUSE-SU-2020:0395

Source: MISC

URL: https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

Source: MLIST

URL: https://lists.apache.org/thread.html/52bafac05ad174000ea465fe275fd3cc7bd5c25535a7631c0bc9bfb2@%3Cuser.flink.apache.org%3E

Name: [flink-user] 20190813 Re: Apache flink 1.7.2 security issues

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2019-08

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2020:0481

Name: RHSA-2020:0481

Source: MISC

URL: https://github.com/jquery/jquery/pull/2588

Source: CONFIRM

URL: https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html

Source: CONFIRM

URL: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: BID

URL: http://www.securityfocus.com/bid/105658

Name: 105658

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2020.html

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2020:0729

Name: RHSA-2020:0729

Source: N/A

URL: https://www.oracle.com/security-alerts/cpuapr2020.html

Name: N/A

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MISC

URL: https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec126.pdf

Source: MISC

URL: https://github.com/jquery/jquery/pull/2588/commits/c254d308a7d3f1eac4d0b42837804cfffcba4bb2

Source: MLIST

URL:
https://lists.apache.org/thread.html/ba79cf1658741e9f146e4c59b50aee56656ea95d841d358d006c18b6@%3Ccommits.roller.apache.org%3E

Name: [roller-commits] 20190820 [jira] [Created] (ROL-2150) Fix Js security vulnerabilities detected using retire js

Source: MLIST

URL:
https://lists.apache.org/thread.html/10f0f3aefd51444d1198c65f44ffdf2d78ca3359423dbc1c168c9731@%3Cdev.flink.apache.org%3E

Name: [flink-dev] 20190811 Apache flink 1.7.2 security issues

Source: MISC

URL: https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

Source: info

URL: http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Source: info

URL: https://nvd.nist.gov/vuln/detail/CVE-2015-9251

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: http://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html

Source: MISC

URL: https://snyk.io/vuln/npm:jquery:20150627

Source: MLIST

URL: https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: CONFIRM

URL: http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html

Source: MISC

URL: https://ics-cert.us-cert.gov/advisories/ICSA-18-212-04

Source: info

URL: https://github.com/jquery/jquery/issues/2432

Source: info

URL: http://research.insecurelabs.org/jquery/test/

Source: MISC

URL: http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html

Source: MISC

URL: https://github.com/jquery/jquery/commit/f60729f3903d17917dc351f3ac87794de379b0cc

Finding 14: jquery:2.1.4 | CVE-2019-11358

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	432

Location

File Path	Line Number
jquery.min.js	None

CVSS v3

None

Description

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable **proto** property, it could extend the native Object.prototype.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/src/main/webapp/js/jquery.min.js

Mitigation

Update jquery:2.1.4 to at least the version recommended in the description

Impact

None

References

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuoct2020.html

Source: MLIST

URL:
https://lists.apache.org/thread.html/r7aac081cbddb6baa24b75e74abf0929bf309b176755a53e3ed810355@%3Cdev.flink.apache.org%3E

Name: [flink-dev] 20200513 [jira] [Created] (FLINK-17675) Resolve CVE-2019-11358 from jquery

Source: MISC

URL: https://github.com/jquery/jquery/pull/4333

Source: MISC

URL: http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2021.html

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/11

Name: 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/Jun/12

Name: 20190612 [SECURITY] [DSA 4460-1] mediawiki security update

Source: MLIST

URL:
https://lists.apache.org/thread.html/r7e8ebccb7c022e41295f6fdb7b971209b83702339f872ddd8cf8bf73@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20200518 [jira] [Updated] (FLINK-17675) Resolve CVE-2019-11358 from jquery

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2019-08

Source: MLIST

URL: https://lists.debian.org/debian-lts-announce/2019/05/msg00029.html

Name: [debian-lts-announce] 20190520 [SECURITY] [DLA 1797-1] drupal7 security update

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/10

Name: 20190510 dotCMS v5.1.1 Vulnerabilities

Source: N/A

URL: https://www.oracle.com/security-alerts/cpuapr2020.html

Name: N/A

Source: MISC

URL: https://www.drupal.org/sa-core-2019-006

Source: MISC

URL: https://backdropcms.org/security/backdrop-sa-core-2019-009

Source: FULLDISC

URL: http://seclists.org/fulldisclosure/2019/May/13

Name: 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

Source: MLIST

URL: https://lists.apache.org/thread.html/bcce5a9c532b386c68dab2f6b3ce8b0cc9b950ec551766e76391caa3@%3Ccommits.nifi.apache.org%3E

Name: [nifi-commits] 20191113 svn commit: r1869773 - /nifi/site/trunk/security.html

Source: MLIST

URL: https://lists.apache.org/thread.html/r41b5bfe009c845f67d4f68948cc9419ac2d62e287804aafd72892b08@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20200518 [jira] [Assigned] (FLINK-17675) Resolve CVE-2019-11358 from jquery

Source: MISC

URL: https://snyk.io/vuln/SNYK-JS-JQUERY-174006

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/5IABSKTYZ5JUGL735UKGXL5YPRYOPUYI/

Name: FEDORA-2019-eba8e44ee6

Source: REDHAT

URL: https://access.redhat.com/errata/RHBA-2019:1570

Name: RHBA-2019:1570

Source: MISC

URL: https://www.privacy-wise.com/mitigating-cve-2019-11358-in-old-versions-of-jquery/

Source: MLIST

URL: https://lists.debian.org/debian-lts-announce/2019/05/msg00006.html

Name: [debian-lts-announce] 20190506 [SECURITY] [DLA 1777-1] jquery security update

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2020-02

Source: MLIST

URL:
https://lists.apache.org/thread.html/r2041a75d3fc09dec55adfd95d598b38d22715303f65c997c054844c9@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20200518 [jira] [Commented] (FLINK-17675) Resolve CVE-2019-11358 from jquery

Source: MISC

URL: http://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html

Source: info

URL: https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Source: MLIST

URL:
https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities

Source: MLIST

URL:
https://lists.apache.org/thread.html/r38f0d1aa3c923c22977fe7376508f030f22e22c1379fbb155bf29766@%3Cdev.syncope.apache.org%3E

Name: [syncope-dev] 20200423 Jquery version on 2.1.x/2.0.x

Source: MLIST

URL:
https://lists.apache.org/thread.html/6097cdbd6f0a337bedd9bb5cc441b2d525ff002a96531de367e4259f@%3Ccommits.airflow.apache.org%3E

Name: [airflow-commits] 20190428 [GitHub] [airflow] XD-DENG commented on issue #5197: [AIRFLOW-XXX] Fix CVE-2019-11358

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00025.html

Name: openSUSE-SU-2019:1872

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: info

URL: https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b

Source: MLIST

URL: https://lists.apache.org/thread.html/5928aa293e39d248266472210c50f176cac1535220f2486e6a7fa844@%3Ccommits.airflow.apache.org%3E

Name: [airflow-commits] 20190428 [GitHub] [airflow] XD-DENG merged pull request #5197: [AIRFLOW-XXX] Fix CVE-2019-11358

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3024

Name: RHSA-2019:3024

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/May/18

Name: 20190509 dotCMS v5.1.1 Vulnerabilities

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:1456

Name: RHSA-2019:1456

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00006.html

Name: openSUSE-SU-2019:1839

Source: MLIST

URL: https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f@%3Cdev.drill.apache.org%3E

Name: [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2022.html

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujul2020.html

Source: BID

URL: http://www.securityfocus.com/bid/108023

Name: 108023

Source: MISC

URL: https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Source: DEBIAN

URL: https://www.debian.org/security/2019/dsa-4460

Name: DSA-4460

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/KYH3OAGR2RTCHRA5NOKX2TES7SNQMWGO/

Name: FEDORA-2019-7eaf0bbe7c

Source: CONFIRM

URL: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601

Source: MLIST

URL: https://lists.apache.org/thread.html/r7d64895cc4dff84d0becfc572b20c0e4bf9bfa7b10c6f5f73e783734@%3Cdev.storm.apache.org%3E

Name: [storm-dev] 20200708 [GitHub] [storm] Crim opened a new pull request #3305: [STORM-3553] Upgrade jQuery from 1.11.1 to 3.5.1

Source: N/A

URL: https://www.oracle.com//security-alerts/cpujul2021.html

Name: N/A

Source: info

URL: https://nvd.nist.gov/vuln/detail/CVE-2019-11358

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WZW27UCJ5CYFL4KFFFMYMIBNMIU2ALG5/

Name: FEDORA-2019-f563e66380

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2020.html

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/RLXRX23725JL366CNZGJZ7AQQB7LHQ6F/

Name: FEDORA-2019-2a0ce0c58c

Source: MISC

URL: https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Source: CONFIRM

URL: https://security.netapp.com/advisory/ntap-20190919-0001/

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/4UOAZIFCSZ3ENEFOR5IXX6NFAD3HV7FA/

Name: FEDORA-2019-1a3edd7e8a

Source: MLIST

URL: https://lists.debian.org/debian-lts-announce/2020/02/msg00024.html

Name: [debian-lts-announce] 20200224 [SECURITY] [DLA 2118-1] otrs2 security update

Source: MLIST

URL:

https://lists.apache.org/thread.html/88fb0362fd40e5b605ea8149f63241537b8b6fb5bfa315391fc5cbb7@%3Ccommits.airflow.apache.org%3E

Name: [airflow-commits] 20190428 [GitHub] [airflow] codecov-io commented on issue #5197: [AIRFLOW-XXX] Fix CVE-2019-11358

Source: MLIST

URL: https://lists.apache.org/thread.html/08720ef215ee7ab3386c05a1a90a7d1c852bf0706f176a7816bf65fc@%3Ccommits.airflow.apache.org%3E

Name: [airflow-commits] 20190428 [GitHub] [airflow] feng-tao commented on issue #5197: [AIRFLOW-XXX] Fix CVE-2019-11358

Source: MLIST

URL: https://lists.apache.org/thread.html/rac25da84ecdcd36f6de5ad0d255f4e967209bbbebddb285e231da37d@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20200513 [jira] [Created] (FLINK-17675) Resolve CVE-2019-11358 from jquery

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:2587

Name: RHSA-2019:2587

Source: MLIST

URL: https://lists.apache.org/thread.html/ba79cf1658741e9f146e4c59b50aee56656ea95d841d358d006c18b6@%3Ccommits.roller.apache.org%3E

Name: [roller-commits] 20190820 [jira] [Created] (ROL-2150) Fix Js security vulnerabilities detected using retire js

Source: MLIST

URL: http://www.openwall.com/lists/oss-security/2019/06/03/2

Name: [oss-security] 20190603 Django: CVE-2019-12308 AdminURLFieldWidget XSS (plus patched bundled jQuery for CVE-2019-11358)

Source: MISC

URL: https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

Source: DEBIAN

URL: https://www.debian.org/security/2019/dsa-4434

Name: DSA-4434

Source: MLIST

URL:
https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc@%3Cissues.drill.apache.org%3E

Name: [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities

Source: MLIST

URL:
https://lists.apache.org/thread.html/r2baacab6e0acb5a2092eb46ae04fd6c3e8277b4fd79b1ffb7f3254fa@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20200520 [jira] [Closed] (FLINK-17675) Resolve CVE-2019-11358 from jquery

Source: MLIST

URL:
https://lists.apache.org/thread.html/b736d0784cf02f5a30fbb4c5902762a15ad6d47e17e2c5a17b7d6205@%3Ccommits.airflow.apache.org%3E

Name: [airflow-commits] 20190428 [GitHub] [airflow] feng-tao opened a new pull request #5197: [AIRFLOW-XXX] Fix CVE-2019-11358

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuoct2021.html

Source: REDHAT

URL: https://access.redhat.com/errata/RHSA-2019:3023

Name: RHSA-2019:3023

Source: MISC

URL: https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b

Source: MLIST

URL:
https://lists.apache.org/thread.html/rca37935d661f4689cb4119f1b3b224413b22be161b678e6e6ce0c69b@%3Ccomm

its.nifi.apache.org%3E

Name: [nifi-commits] 20200123 svn commit: r1873083 - /nifi/site/trunk/security.html

Source: CONFIRM

URL: https://www.synology.com/security/advisory/Synology_SA_19_19

Source: BUGTRAQ

URL: https://seclists.org/bugtraq/2019/Apr/32

Name: 20190421 [SECURITY] [DSA 4434-1] drupal7 security update

Source: MISC

URL: http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QV3PKZC3PQCO3273HAT76PAQZFBEO4KP/

Name: FEDORA-2019-a06dffab1c

Finding 15: jquery:2.1.4 | CVE-2020-11022

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	433

Location

File Path	Line Number
jquery.min.js	None

CVSS v3

None

Description

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/src/main/webapp/js/jquery.min.js

Mitigation

Update jquery:2.1.4 to at least the version recommended in the description

Impact

None

References

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuoct2020.html

Source: MLIST

URL: https://lists.apache.org/thread.html/r54565a8f025c7c4f305355fdfd75b68eca442eebdb5f31c2e7d977ae@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210429 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2022.html

Source: MLIST

URL: https://lists.apache.org/thread.html/ree3bd8ddb23df5fa4e372d11c226830ea3650056b1059f3965b3fce2@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210422 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujul2020.html

Source: MISC

URL: https://jquery.com/upgrade-guide/3.5/

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AVKYXLWCLZBV2N7M46KYK4LVA5OXWPBY/

Name: FEDORA-2020-0b32a59b54

Source: MLIST

URL: https://lists.apache.org/thread.html/rede9cfaa756e050a3d83045008f84a62802fc68c17f2b4eabeaae5e4@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210422 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: GENTOO

URL: https://security.gentoo.org/glsa/202007-03

Name: GLSA-202007-03

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QPN2L2XVQGUA2V5HNQJWHK3APSK3VN7K/

Name: FEDORA-2020-36d2db5f51

Source: MISC

URL: https://github.com/jquery/jquery/commit/1d61fd9407e6fbe82fe55cb0b938307aa0791f77

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2020-11/msg00039.html

Name: openSUSE-SU-2020:1888

Source: DEBIAN

URL: https://www.debian.org/security/2020/dsa-4693

Name: DSA-4693

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2021.html

Source: MLIST

URL:

https://lists.apache.org/thread.html/r49ce4243b4738dd763caeb27fa8ad6afb426ae3e8c011ff00b8b1f48@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20201129 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: CONFIRM

URL: https://security.netapp.com/advisory/ntap-20200511-0006/

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-02

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VOE7P7APPRQKD4FGNHBKJPDY6FFCOH3W/

Name: FEDORA-2020-11be4b36d4

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00067.html

Name: openSUSE-SU-2020:1060

Source: CONFIRM

URL: https://www.drupal.org/sa-core-2020-002

Source: MLIST

URL:
https://lists.apache.org/thread.html/r0483ba0072783c2e1bfea613984bfb3c86e73ba8879d780dc1cc7d36@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20211031 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MLIST

URL:
https://lists.apache.org/thread.html/r8f70b0f65d6bedf316ecd899371fd89e65333bc988f6326d2956735c@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210209 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: N/A

URL: https://www.oracle.com//security-alerts/cpujul2021.html

Name: N/A

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-10

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SFP4UK4EGP4AFH2MWYJ5A5Z4I7XVFQ6B/

Name: FEDORA-2020-fbb94073a1

Source: MLIST

URL: https://lists.apache.org/thread.html/r706cfbc098420f7113968cc377247ec3d1439bce42e679c11c609e2d@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MISC

URL: http://packetstormsecurity.com/files/162159/jQuery-1.2-Cross-Site-Scripting.html

Source: MLIST

URL: https://lists.apache.org/thread.html/rdf44341677cf7eec7e9aa96dcf3f37ed709544863d619cca8c36f133@%3Ccommits.airflow.apache.org%3E

Name: [airflow-commits] 20200820 [GitHub] [airflow] breser opened a new issue #10429: jquery dependency needs to be updated to 3.5.0 or newer

Source: MLIST

URL: https://lists.apache.org/thread.html/r564585d97bc069137e64f521e68ba490c7c9c5b342df5d73c49a0760@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210209 [jira] [Comment Edited] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MLIST

URL: https://lists.debian.org/debian-lts-announce/2021/03/msg00033.html

Name: [debian-lts-announce] 20210326 [SECURITY] [DLA 2608-1] jquery security update

Source: MLIST

URL: https://lists.apache.org/thread.html/rbb448222ba62c430e21e13f940be4cb5cfc373cd3bce56b48c0ffa67@%3Cdev.flink.apache.org%3E

Name: [flink-dev] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuoct2021.html

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00085.html

Name: openSUSE-SU-2020:1106

Source: CONFIRM

URL: https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2

Source: MISC

URL: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2020-11

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2020-10

Source: info

URL: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SAPQVX3XDNPGFT26QAQ6AJIXZZBZ4CD4/

Name: FEDORA-2020-fe94df8c34

Source: MLIST

URL: https://lists.apache.org/thread.html/re4ae96fa5c1a2fe71ccbb7b7ac1538bd0cb677be270a2bf6e2f8d108@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210429 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Finding 16: jquery:2.1.4 | CVE-2020-11023

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	Active, Verified	March 27, 2022	1 days	(admin)	79 (https://cwe.mitre.org/data/definitions/79.html)	434

Location

File Path	Line Number
jquery.min.js	None

CVSS v3

None

Description

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Source: NVD

Filepath: /builds/xokage/BenchmarkJava/src/main/webapp/js/jquery.min.js

Mitigation

Update jquery:2.1.4 to at least the version recommended in the description

Impact

None

References

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuoct2020.html

Source: MLIST

URL:
https://lists.apache.org/thread.html/r9006ad2abf81d02a0ef2126bab5177987e59095b7194a487c4ea247c@%3Ccommits.felix.apache.org%3E

Name: [felix-commits] 20201208 [felix-dev] branch master updated: FELIX-6366 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023 (#64)

Source: MLIST

URL:
https://lists.apache.org/thread.html/r54565a8f025c7c4f305355fdfd75b68eca442eebdb5f31c2e7d977ae@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210429 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AVKYXLWCLZBV2N7M46KYK4LVA5OXWPBY/

Name: FEDORA-2020-0b32a59b54

Source: MLIST

URL:
https://lists.apache.org/thread.html/r4dba67be3239b34861f1b9cfdf9dfb3a90272585dcce374112ed6e16@%3Cdev.felix.apache.org%3E

Name: [felix-dev] 20201208 [jira] [Updated] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QPN2L2XVQGUA2V5HNQJWHK3APSK3VN7K/

Name: FEDORA-2020-36d2db5f51

Source: MLIST

URL:
https://lists.apache.org/thread.html/rb69b7d8217c1a6a2100247a5d06ce610836b31e3f5d73fc113ded8e7@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200902 [jira] [Comment Edited] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL: https://lists.apache.org/thread.html/r4aadb98086ca72ed75391f54167522d91489a0d0ae25b12baa8fc7c5@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200904 [jira] [Assigned] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL: https://lists.apache.org/thread.html/r9e0bd31b7da9e7403478d22652b8760c946861f8ebd7bd750844898e@%3Cdev.felix.apache.org%3E

Name: [felix-dev] 20201208 [jira] [Commented] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023

Source: MLIST

URL: https://lists.apache.org/thread.html/r6c4df3b33e625a44471009a172dabe6865faec8d8f21cac2303463b1@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200915 [jira] [Work logged] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2021.html

Source: CONFIRM

URL: https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-02

Source: MLIST

URL: https://lists.apache.org/thread.html/r0593393ca1e97b1e7e098fe69d414d6bd0a467148e9138d07e86ebbb@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200915 [jira] [Updated] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/ra374bb0299b4aa3e04edde01ebc03ed6f90cf614dad40dd428ce8f72@%3Cgitbox.hive.apache.org%3E

Name: [hive-gitbox] 20200911 [GitHub] [hive] rajkrrsingh closed pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/r8f70b0f65d6bedf316ecd899371fd89e65333bc988f6326d2956735c@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210209 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MLIST

URL:
https://lists.apache.org/thread.html/ra406b3adfcffcb5ce8707013bdb7c35e3ffc2776a8a99022f15274c6@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200915 [jira] [Resolved] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/rf661a90a15da8da5922ba6127b3f5f8194d4ebec8855d60a0dd13248@%3Cdev.hive.apache.org%3E

Name: [hive-dev] 20200813 [jira] [Created] (HIVE-24039) update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/rf0f8939596081d84be1ae6a91d6248b96a02d8388898c372ac807817@%3Cdev.felix.apache.org%3E

Name: [felix-dev] 20201208 [jira] [Assigned] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/r564585d97bc069137e64f521e68ba490c7c9c5b342df5d73c49a0760@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210209 [jira] [Comment Edited] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00085.html

Name: openSUSE-SU-2020:1106

Source: MLIST

URL:
https://lists.apache.org/thread.html/rd38b4185a797b324c8dd940d9213cf99fcdc2dbf1fc5a63ba7dee8c9@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200902 [jira] [Commented] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MISC

URL: http://packetstormsecurity.com/files/162160/jQuery-1.0.3-Cross-Site-Scripting.html

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuApr2021.html

Source: MLIST

URL:
https://lists.apache.org/thread.html/r3702ede0ff83a29ba3eb418f6f11c473d6e3736baba981a8dbd9c9ef@%3Cdev.felix.apache.org%3E

Name: [felix-dev] 20201208 [GitHub] [felix-dev] cziegeler merged pull request #64: FELIX-6366 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/r9c5fda81e4bca8daee305b4c03283dddb383ab8428a151d4cb0b3b15@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200813 [jira] [Updated] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SAPQVX3XDNPGFT26QAQ6AJIXZZBZ4CD4/

Name: FEDORA-2020-fe94df8c34

Source: MLIST

URL:

https://lists.apache.org/thread.html/re4ae96fa5c1a2fe71ccbb7b7ac1538bd0cb677be270a2bf6e2f8d108@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210429 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MLIST

URL:
https://lists.apache.org/thread.html/rb25c3bc7418ae75cba07988dafe1b6912f76a9dd7d94757878320d61@%3Cgitbox.hive.apache.org%3E

Name: [hive-gitbox] 20200911 [GitHub] [hive] rajkrrsingh opened a new pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujan2022.html

Source: MLIST

URL:
https://lists.apache.org/thread.html/radcb2aa874a79647789f3563fcbbceaf1045a029ee8806b59812a8ea@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200902 [jira] [Work started] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/r55f5e066cc7301e3630ce90bbbf8d28c82212ae1f2d4871012141494@%3Cdev.felix.apache.org%3E

Name: [felix-dev] 20201208 [jira] [Updated] (FELIX-6366) 1.0.3 < jQuery <3.5.0 is vulnerable to CVE-2020-11023

Source: MLIST

URL:
https://lists.apache.org/thread.html/ree3bd8ddb23df5fa4e372d11c226830ea3650056b1059f3965b3fce2@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210422 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MISC

URL: https://www.oracle.com/security-alerts/cpujul2020.html

Source: MLIST

URL: https://lists.apache.org/thread.html/ra3c9219fcb0b289e18e9ec5a5ebeaa5c17d6b79a201667675af6721c@%3Cgitbox.hive.apache.org%3E

Name: [hive-gitbox] 20200813 [GitHub] [hive] rajkrrsingh opened a new pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023

Source: MISC

URL: https://jquery.com/upgrade-guide/3.5/

Source: MLIST

URL: https://lists.apache.org/thread.html/rab82dd040f302018c85bd07d33f5604113573514895ada523c3401d9@%3Ccommits.hive.apache.org%3E

Name: [hive-commits] 20200915 [hive] branch master updated: HIVE-24039 : Update jquery version to mitigate CVE-2020-11023 (#1403)

Source: MLIST

URL: https://lists.apache.org/thread.html/r094f435595582f6b5b24b66fedf80543aa8b1d57a3688fbcc21f06ec@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200813 [jira] [Assigned] (HIVE-24039) update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL: https://lists.apache.org/thread.html/rede9cfaa756e050a3d83045008f84a62802fc68c17f2b4eabeaae5e4@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20210422 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: GENTOO

URL: https://security.gentoo.org/glsa/202007-03

Name: GLSA-202007-03

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2020-11/msg00039.html

Name: openSUSE-SU-2020:1888

Source: DEBIAN

URL: https://www.debian.org/security/2020/dsa-4693

Name: DSA-4693

Source: MLIST

URL: https://lists.apache.org/thread.html/r49ce4243b4738dd763caeb27fa8ad6afb426ae3e8c011ff00b8b1f48@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20201129 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: CONFIRM

URL: https://security.netapp.com/advisory/ntap-20200511-0006/

Source: MLIST

URL: https://lists.apache.org/thread.html/r1fed19c860a0d470f2a3eded12795772c8651ff583ef951ddac4918c@%3Cgitbox.hive.apache.org%3E

Name: [hive-gitbox] 20200915 [GitHub] [hive] kgyrtkirk merged pull request #1403: HIVE-24039 : Update jquery version to mitigate CVE-2020-11023

Source: SUSE

URL: http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00067.html

Name: openSUSE-SU-2020:1060

Source: CONFIRM

URL: https://www.drupal.org/sa-core-2020-002

Source: MLIST

URL: https://lists.apache.org/thread.html/rf1ba79e564fe7efc56aef7c986106f1cf67a3427d08e997e088e7a93@%3Cgitbox.hive.apache.org%3E

Name: [hive-gitbox] 20200912 [GitHub] [hive] rajkrrsingh closed pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL: https://lists.apache.org/thread.html/r0483ba0072783c2e1bfea613984bfb3c86e73ba8879d780dc1cc7d36@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20211031 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MLIST

URL: https://lists.apache.org/thread.html/r2c85121a47442036c7f8353a3724aa04f8ecdfda1819d311ba4f5330@%3Cdev.felix.apache.org%3E

Name: [felix-dev] 20201208 [jira] [Created] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023

Source: N/A

URL: https://www.oracle.com//security-alerts/cpujul2021.html

Name: N/A

Source: CONFIRM

URL: https://www.tenable.com/security/tns-2021-10

Source: FEDORA

URL: https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/SFP4UK4EGP4AFH2MWYJ5A5Z4I7XVFQ6B/

Name: FEDORA-2020-fbb94073a1

Source: MLIST

URL: https://lists.apache.org/thread.html/rda99599896c3667f2cc9e9d34c7b6ef5d2bbed1f4801e1d75a2b0679@%3Ccommits.nifi.apache.org%3E

Name: [nifi-commits] 20200930 svn commit: r1882168 - /nifi/site/trunk/security.html

Source: MLIST

URL: https://lists.apache.org/thread.html/r706cfbc098420f7113968cc377247ec3d1439bce42e679c11c609e2d@%3Cissues.flink.apache.org%3E

Name: [flink-issues] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MLIST

URL: https://lists.apache.org/thread.html/r07ab379471fb15644bf7a92e4a98cbc7df3cf4e736abae0cc7625fe6@%3Cdev.felix.apache.org%3E

Name: [felix-dev] 20201208 [GitHub] [felix-dev] abhishekgarg18 opened a new pull request #64: FELIX-6366 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023

Source: MLIST

URL: https://lists.debian.org/debian-lts-announce/2021/03/msg00033.html

Name: [debian-lts-announce] 20210326 [SECURITY] [DLA 2608-1] jquery security update

Source: MLIST

URL: https://lists.apache.org/thread.html/r6e97b37963926f6059ecc1e417721608723a807a76af41d4e9dbed49@%3Cissues.hive.apache.org%3E

Name: [hive-issues] 20200902 [jira] [Assigned] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

Source: MLIST

URL: https://lists.apache.org/thread.html/rbb448222ba62c430e21e13f940be4cb5cfc373cd3bce56b48c0ffa67@%3Cdev.flink.apache.org%3E

Name: [flink-dev] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler

Source: MISC

URL: https://www.oracle.com/security-alerts/cpuoct2021.html

Source: MLIST

URL: https://lists.apache.org/thread.html/ra32c7103ded9041c7c1cb8c12c8d125a6b2f3f3270e2937ef8417fac@%3Cgitbox.hive.apache.org%3E

Name: [hive-gitbox] 20200912 [GitHub] [hive] rajkrrsingh opened a new pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023

Source: MISC

URL: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released

Source: info

URL: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Low

Finding 17: javascript.lang.correctness.no-replaceall.no-replaceall

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	850

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/src/main/webapp/js/testsuiteutils.js	164

CVSS v3

None

Description

Result message: The string method replaceAll is not supported in all versions of javascript, and is not supported by older browser versions. Consider using replace() with a regex as the first argument instead like mystring.replace(/bad/g, "good") instead of mystring.replaceAll("bad", "good") (https://discourse.threejs.org/t/replaceall-is-not-a-function/14585)

Snippet:

```
result = result.replaceAll("<br>", "\n"); // Replace all <br>'s with carriage returns'
```

Mitigation

None

Impact

None

Finding 18: javascript.lang.correctness.no-replaceall.no-replaceall

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	851

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/src/main/webapp/js/testsuiteutils.js	196

CVSS v3

None

Description

Result message: The string method replaceAll is not supported in all versions of javascript, and is not supported by older browser versions. Consider using replace() with a regex as the first argument instead like mystring.replace(/bad/g, "good") instead of mystring.replaceAll("bad", "good") (https://discourse.threejs.org/t/replaceall-is-not-a-function/14585)

Snippet:

```
var result = xmlResponse.replaceAll('<?xml version="1.0" encoding="UTF-8" standalone="yes"?>', "");
```

Mitigation

None

Impact

None

Finding 19: javascript.lang.correctness.no-replaceall.no-replaceall

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	852

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/src/main/webapp/js/testsuiteutils.js	197

CVSS v3

None

Description

Result message: The string method replaceAll is not supported in all versions of javascript, and is not supported by older browser versions. Consider using replace() with a regex as the first argument instead like mystring.replace(/bad/g, "good") instead of mystring.replaceAll("bad", "good")

(https://discourse.threejs.org/t/replaceall-is-not-a-function/14585)

Snippet:

```
result = result.replaceAll("<xMLMessages>","").replaceAll("</xMLMessages>","").replaceAll("<message><msg>","");
```

Mitigation

None

Impact

None

Finding 20: javascript.lang.correctness.no-replaceall.no-replaceall

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	853

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/src/main/webapp/js/testsuiteutils.js	198

CVSS v3

None

Description

Result message: The string method replaceAll is not supported in all versions of javascript, and is not supported by older browser versions. Consider using replace() with a regex as the first argument instead like mystring.replace(/bad/g, "good") instead of mystring.replaceAll("bad", "good") (https://discourse.threejs.org/t/replaceall-is-not-a-function/14585)

Snippet:

```
result = result.replaceAll("</msg></message>","\n");
```

Mitigation

None

Impact

None

Finding 21: javascript.lang.correctness.no-replaceall.no-replaceall

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	854

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/src/main/webapp/js/testsuiteutils.js	248

CVSS v3

None

Description

Result message: The string method replaceAll is not supported in all versions of javascript, and is not supported by older browser versions. Consider using replace() with a regex as the first argument instead like mystring.replace(/bad/g, "good") instead of mystring.replaceAll("bad", "good") (https://discourse.threejs.org/t/replaceall-is-not-a-function/14585)

Snippet:

msgString = msgString.substring(prefix.length, msgString.length - 2).replaceAll("\\n", "\n");

Mitigation

None

Impact

None

Finding 22: javascript.lang.best-practice.leftover_debugging.javascript-alert

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	855

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/src/main/webapp/js/testsuiteutils.js	190

CVSS v3

None

Description

Result message: found alert() call; should this be in production code?

Snippet:

```
error: function (xhr, textStatus, errorThrown){ alert(errorThrown); }
```

Mitigation

None

Impact

None

Finding 23: javascript.lang.best-practice.leftover_debugging.javascript-alert

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	856

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/src/main/webapp/js/testsuiteutils.js	238

CVSS v3

None

Description

Result message: found alert() call; should this be in production code?

Snippet:

```
error: function (xhr, textStatus, errorThrown){ alert(errorThrown);}
```

Mitigation

None

Impact

None

Finding 24: generic.dockerfile.best-practice.set-pipefail.set-pipefail

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	857

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/VMs/Dockerfile	23

CVSS v3

None

Description

Result message: Only the exit code from the final command in this RUN instruction will be evaluated unless 'pipefail' is set. If you want to fail the command at any stage in the pipe, set 'pipefail' by including 'SHELL ["/bin/bash", "-o", "pipefail", "-c"] before the command. If you're using alpine and don't have bash installed, communicate this explicitly with SHELL ["/bin/ash"].

Snippet:

RUN echo bench:bench | chpasswd

Mitigation

None

Impact

None

References

https://github.com/hadolint/hadolint/wiki/DL4006

Finding 25: generic.dockerfile.best-practice.remove-package-lists.remove-package-lists

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	858

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/VMs/Dockerfile	5

CVSS v3

None

Description

Result message: The package lists were not deleted after running 'apt-get update', which increases the size of the image. Remove the package lists by appending '&& rm -rf /var/lib/apt/lists/ _' at the end of apt-get command chain._

Snippet:*

RUN apt-get update

Mitigation

None

Impact

None

References

https://github.com/hadolint/hadolint/wiki/DL3009

Finding 26: generic.dockerfile.best-practice.avoid-latest-version.avoid-latest-version

Severity	Status	Date discovered	Age	Reporter	Dojo ID
Low	Active, Verified	March 27, 2022	1 days	(admin)	859

Location

File Path	Line Number
/builds/xokage/BenchmarkJava/VMs/Dockerfile	2

CVSS v3

None

Description

Result message: Images should be tagged with an explicit version to produce deterministic container images. The 'latest' tag may change the base container without warning.

Snippet:

FROM ubuntu:latest

Mitigation

None

Impact

None

References

https://github.com/hadolint/hadolint/wiki/DL3007

Finding 27: java.lang.security.audit.crypto.des-is-deprecated.des-is-deprecated

Severity	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Low						