How to read the report | Suppressing false positives | **Getting Help:** github issues

Sponsor

Project: Fusion Registry

Scan Information (show all):

- *dependency-check version*: 6.1.6
- *Report Generated On*: Wed, 12 May 2021 09:15:11 +0100
- *Dependencies Scanned*: 1201 (1158 unique)
- *Vulnerable Dependencies*: 5
- *Vulnerabilities Found*: 17
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
FusionRegistry.war: FusionDataBrowser-2.0.5.jar: bootstrap.bundle.min.js		pkg:javascript/bootstrap@4.0.0-dist%5Cjs%5Cbootstrap.bundle.min	MEDIUM	4		3
FusionRegistry.war: FusionDataBrowser-2.0.5.jar: jquery.min.js		pkg:javascript/jquery@3.3.1	MEDIUM	3		3
FusionRegistry.war: bootstrap.min.js		pkg:javascript/bootstrap@3.3.5	MEDIUM	4		3
FusionRegistry.war: commons-io-2.6.jar	cpe:2.3:a:apache:commons_io:2.6:*:*:*:*:*:*:*	pkg:maven/commons-io/commons-io@2.6	MEDIUM	1	Highest	40
FusionRegistry.war: spring-rabbit-2.3.6.jar	cpe:2.3:a:pivotal_software:rabbitmq:2.3.6:*:*:*:*:*:*:*	pkg:maven/org.springframework.amqp/spring-rabbit@2.3.6	MEDIUM	5	Low	38

Dependencies

FusionRegistry.war: FusionDataBrowser-2.0.5.jar: bootstrap.bundle.min.js

File Path: F:\tomcats\apache-tomcat-9.0.44\webapps\FusionRegistry.war\WEB-INF\lib\FusionDataBrowser-2.0.5.jar\databrowser\assets\js\vendor\bootstrap-4.0.0-dist\js\bootstrap.bundle.min.js
MD5: fb63ebd7050580f171cb88b16f94e00c
SHA1: 6273d84ca0d1103af58ecde686db443596835dfc
SHA256:e6249266ea92f60bbb67c338022758e4f5adfbcac60c4d57dd16a9b25f489343

Evidence

Identifiers

- pkg:javascript/bootstrap@4.0.0-dist%5Cjs%5Cbootstrap.bundle.min (*Confidence*:Highest)

Published Vulnerabilities

CVE-2018-14040 suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)

- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/
- MISC - https://github.com/twbs/bootstrap/issues/26423
- MISC - https://github.com/twbs/bootstrap/issues/26625
- MISC - https://github.com/twbs/bootstrap/pull/26630
- MLIST - [debian-lts-announce] 20180827 [SECURITY] [DLA 1479-1] twitter-bootstrap3 security update
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- info - https://github.com/twbs/bootstrap/issues/20184

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.0.0; versions up to (excluding) 4.1.2
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.0
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*

CVE-2018-14041 suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/
- MISC - https://github.com/twbs/bootstrap/issues/26423
- MISC - https://github.com/twbs/bootstrap/issues/26627
- MISC - https://github.com/twbs/bootstrap/pull/26630
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- REDHAT - RHSA-2019:1456
- info - https://github.com/twbs/bootstrap/issues/20184

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.0.0; versions up to (excluding) 4.1.2
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*

CVE-2018-14042 suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:

- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/
- MISC - https://github.com/twbs/bootstrap/issues/26423
- MISC - https://github.com/twbs/bootstrap/issues/26628
- MISC - https://github.com/twbs/bootstrap/pull/26630
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- info - https://github.com/twbs/bootstrap/issues/20184

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.0.0; versions up to (excluding) 4.1.2
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.0
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*

CVE-2019-8331 suppress

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.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BID - 107375
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- CONFIRM - https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/
- CONFIRM - https://support.f5.com/csp/article/K24383845
- CONFIRM - https://support.f5.com/csp/article/K24383845?utm_source=f5support&utm_medium=RSS
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://github.com/twbs/bootstrap/pull/28236
- MISC - https://github.com/twbs/bootstrap/releases/tag/v3.4.1
- MISC - https://github.com/twbs/bootstrap/releases/tag/v4.3.1
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [flink-dev] 20190811 Apache flink 1.7.2 security issues
- MLIST - [flink-user] 20190811 Apache flink 1.7.2 security issues
- MLIST - [flink-user] 20190813 Apache flink 1.7.2 security issues
- MLIST - [flink-user] 20190813 Re: Apache flink 1.7.2 security issues
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- REDHAT - RHSA-2019:1456
- REDHAT - RHSA-2019:3023
- REDHAT - RHSA-2019:3024
- info - https://github.com/twbs/bootstrap/issues/28236

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.3.0; versions up to (excluding) 4.3.1
- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0

- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:redhat:virtualization_manager:4.3:*:*:*:*:*:*:*
- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.1
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5

FusionRegistry.war: FusionDataBrowser-2.0.5.jar: jquery.min.js

File Path: F:\tomcats\apache-tomcat-9.0.44\webapps\FusionRegistry.war\WEB-INF\lib\FusionDataBrowser-2.0.5.jar\databrowser\assets\js\vendor\jquery\jquery.min.js
MD5: a09e13ee94d51c524b7e2a728c7d4039
SHA1: 0dc32db4aa9c5f03f3b38c47d883dbd4fed13aae
SHA256:160a426ff2894252cd7cebbdd6d6b7da8fcd319c65b70468f10b6690c45d02ef

Evidence

Identifiers

- pkg:javascript/jquery@3.3.1 (*Confidence*:Highest)

Published Vulnerabilities

CVE-2019-11358 suppress

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.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BID - 108023
- BUGTRAQ - 20190421 [SECURITY] [DSA 4434-1] drupal7 security update
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- BUGTRAQ - 20190612 [SECURITY] [DSA 4460-1] mediawiki security update
- CONFIRM - https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601
- CONFIRM - https://security.netapp.com/advisory/ntap-20190919-0001/
- CONFIRM - https://www.synology.com/security/advisory/Synology_SA_19_19
- CONFIRM - https://www.tenable.com/security/tns-2019-08
- CONFIRM - https://www.tenable.com/security/tns-2020-02
- DEBIAN - DSA-4434
- DEBIAN - DSA-4460
- FEDORA - FEDORA-2019-1a3edd7e8a
- FEDORA - FEDORA-2019-2a0ce0c58c
- FEDORA - FEDORA-2019-7eaf0bbe7c
- FEDORA - FEDORA-2019-a06dffab1c
- FEDORA - FEDORA-2019-eba8e44ee6
- FEDORA - FEDORA-2019-f563e66380
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability

- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
- MISC - http://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://backdropcms.org/security/backdrop-sa-core-2019-009
- MISC - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
- MISC - https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b
- MISC - https://github.com/jquery/jquery/pull/4333
- MISC - https://snyk.io/vuln/SNYK-JS-JQUERY-174006
- MISC - https://www.drupal.org/sa-core-2019-006
- MISC - https://www.oracle.com/security-alerts/cpujan2020.html
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MISC - https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
- MISC - https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
- MISC - https://www.privacy-wise.com/mitigating-cve-2019-11358-in-old-versions-of-jquery/
- MLIST - [airflow-commits] 20190428 [GitHub] [airflow] XD-DENG commented on issue #5197: [AIRFLOW-XXX] Fix CVE-2019-11358
- MLIST - [airflow-commits] 20190428 [GitHub] [airflow] XD-DENG merged pull request #5197: [AIRFLOW-XXX] Fix CVE-2019-11358
- MLIST - [airflow-commits] 20190428 [GitHub] [airflow] codecov-io commented on issue #5197: [AIRFLOW-XXX] Fix CVE-2019-11358
- MLIST - [airflow-commits] 20190428 [GitHub] [airflow] feng-tao commented on issue #5197: [AIRFLOW-XXX] Fix CVE-2019-11358
- MLIST - [airflow-commits] 20190428 [GitHub] [airflow] feng-tao opened a new pull request #5197: [AIRFLOW-XXX] Fix CVE-2019-11358
- MLIST - [debian-lts-announce] 20190506 [SECURITY] [DLA 1777-1] jquery security update
- MLIST - [debian-lts-announce] 20190520 [SECURITY] [DLA 1797-1] drupal7 security update
- MLIST - [debian-lts-announce] 20200224 [SECURITY] [DLA 2118-1] otrs2 security update
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [flink-dev] 20200513 [jira] [Created] (FLINK-17675) Resolve CVE-2019-11358 from jquery
- MLIST - [flink-issues] 20200513 [jira] [Created] (FLINK-17675) Resolve CVE-2019-11358 from jquery
- MLIST - [flink-issues] 20200518 [jira] [Assigned] (FLINK-17675) Resolve CVE-2019-11358 from jquery
- MLIST - [flink-issues] 20200518 [jira] [Commented] (FLINK-17675) Resolve CVE-2019-11358 from jquery
- MLIST - [flink-issues] 20200518 [jira] [Updated] (FLINK-17675) Resolve CVE-2019-11358 from jquery
- MLIST - [flink-issues] 20200520 [jira] [Closed] (FLINK-17675) Resolve CVE-2019-11358 from jquery
- MLIST - [nifi-commits] 20191113 svn commit: r1869773 - /nifi/site/trunk/security.html
- MLIST - [nifi-commits] 20200123 svn commit: r1873083 - /nifi/site/trunk/security.html
- MLIST - [oss-security] 20190603 Django: CVE-2019-12308 AdminURLFieldWidget XSS (plus patched bundled jQuery for CVE-2019-11358)
- MLIST - [roller-commits] 20190820 [jira] [Created] (ROL-2150) Fix Js security vulnerabilities detected using retire js
- MLIST - [storm-dev] 20200708 [GitHub] [storm] Crim opened a new pull request #3305: [STORM-3553] Upgrade jQuery from 1.11.1 to 3.5.1
- MLIST - [syncope-dev] 20200423 Jquery version on 2.1.x/2.0.x
- N/A - N/A
- REDHAT - RHBA-2019:1570
- REDHAT - RHSA-2019:1456
- REDHAT - RHSA-2019:2587
- REDHAT - RHSA-2019:3023
- REDHAT - RHSA-2019:3024
- SUSE - openSUSE-SU-2019:1839
- SUSE - openSUSE-SU-2019:1872
- info - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
- info - https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b
- info - https://nvd.nist.gov/vuln/detail/CVE-2019-11358

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:oracle:communications_billing_and_revenue_management:7.5.0.23.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_materials_control:18.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:12.1.0.2:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:big_data_discovery:1.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation_connector_for_siebel:10.4.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_report_manager:8.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_analytical_applications_infrastructure:*:*:*:*:*:*:*:* versions from (including) 7.3.3; versions up to (including) 7.3.5
- cpe:2.3:a:oracle:financial_services_enterprise_financial_performance_analytics:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:enterprise_manager_ops_center:12.3.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_guest_access:4.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 16.2.0; versions up to (including) 16.2.11
- cpe:2.3:a:oracle:financial_services_retail_performance_analytics:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation:12.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_allocation_manager_for_enterprise_profitability:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 8.5.0; versions up to (excluding) 8.5.15
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_internal_ratings_based_approach:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:financial_services_profitability_management:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_accounting_analyzer:8.0.9:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:agile_product_lifecycle_management_for_process:6.2.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:enterprise_session_border_controller:8.4:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_analytical_applications_reconciliation_framework:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 8.6.0; versions up to (excluding) 8.6.15
- cpe:2.3:a:oracle:communications_diameter_signaling_router:8.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_funds_transfer_pricing:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_application_session_controller:3.8m0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_data_integration_hub:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jdeveloper:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_unifier:16.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_billing_and_revenue_management:12.0.0.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_translational_research:3.3.1:*:*:*:*:*:*:*
- cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*
- cpe:2.3:a:oracle:tape_library_acsls:8.5:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:bi_publisher:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.56:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jdeveloper:11.1.1.9.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.57:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_interactive_session_recorder:*:*:*:*:*:*:*:* versions from (including) 6.0; versions up to (including) 6.4
- cpe:2.3:a:oracle:financial_services_balance_sheet_planning:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_management:8.0.2:*:*:*:*:*:*:*

- cpe:2.3:a:oracle:insurance_insbridge_rating_and_underwriting:5.6.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation:*:*:*:*:*:*:*:* versions from (including) 12.2.0; versions up to (including) 12.2.15
- cpe:2.3:a:oracle:financial_services_funds_transfer_pricing:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:financial_services_liquidity_risk_measurement_and_management:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_customer_insights:15.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_simphony:18.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_testing_suite:12.5.0.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_asset_liability_management:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:banking_digital_experience:20.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation_for_mobile_devices:*:*:*:*:*:*:*:* versions from (including) 12.2.0; versions up to (including) 12.2.15
- cpe:2.3:a:oracle:financial_services_retail_performance_analytics:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_point-of-service:14.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_express:*:*:*:*:*:*:*:* versions up to (excluding) 19.1
- cpe:2.3:a:oracle:application_testing_suite:13.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_testing_suite:13.1.0.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_diameter_signaling_router:8.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_element_manager:8.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_element_manager:8.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_foundation:7.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:18c:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:financial_services_regulatory_reporting_for_us_federal_reserve:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:communications_session_report_manager:8.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_billing_and_revenue_management:12.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:transportation_management:1.4.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_analytics:12.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_institutional_performance_analytics:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:financial_services_analytical_applications_infrastructure:*:*:*:*:*:*:*:* versions from (including) 8.0.2; versions up to (including) 8.1.0
- cpe:2.3:a:oracle:enterprise_manager_ops_center:12.4.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_route_manager:8.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_guest_access:4.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jdeveloper_and_adf:12.1.3.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_customer_insights:16.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_loan_loss_forecasting_and_provisioning:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:redhat:virtualization_manager:4.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:business_process_management_suite:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_hedge_management_and_ifrs_valuations:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:banking_digital_experience:18.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_allocation_manager_for_enterprise_profitability:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_unifier:18.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_revenue_management_and_billing:2.4.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:19c:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:tape_library_acsls:8.5.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_regulatory_reporting_for_european_banking_authority:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_foundation:7.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_ifrs_17_analyzer:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:real-time_scheduler:*:*:*:*:*:*:*:* versions from (including) 2.3.0.1; versions up to (including) 2.3.0.3
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 18.8.0; versions up to (including) 18.8.9
- cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_retail_customer_analytics:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.6
- cpe:2.3:a:oracle:business_process_management_suite:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_central_office:14.1:*:*:*:*:*:*:*
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 7.0; versions up to (excluding) 7.66
- cpe:2.3:a:netapp:snapcenter:-:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_digital_experience:19.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_enterprise_collections:*:*:*:*:*:*:*:* versions from (including) 2.7.0; versions up to (including) 2.8.0
- cpe:2.3:a:oracle:retail_returns_management:14.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_management:8.0.0.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_foundation:7.2.2:*:*:*:*:*:*:*
- cpe:2.3:a:redhat:cloudforms:4.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation:12.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_regulatory_reporting_for_de_nederlandsche_bank:8.0.4:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_unified_inventory_management:7.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:agile_product_lifecycle_management_for_process:6.2.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_management:8.0.4.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_operations_monitor:4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_analytical_applications_reconciliation_framework:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_enterprise_financial_performance_analytics:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:enterprise_manager_ops_center:12.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_loan_loss_forecasting_and_provisioning:*:*:*:*:*:*:*:* versions from (including) 8.0.2; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:communications_webrtc_session_controller:7.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_revenue_management_and_billing:2.4.0.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_operations_monitor:3.4:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:service_bus:12.1.3.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_institutional_performance_analytics:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:12.2.0.1:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:financial_services_market_risk_measurement_and_management:8.0.5:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_translational_research:3.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_service_level_management:13.2.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:service_bus:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_digital_experience:18.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_translational_research:3.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_basic:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_measurement_and_management:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_element_manager:8.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation:10.4.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:knowledge:*:*:*:*:*:*:*:* versions from (including) 8.6.0; versions up to (including) 8.6.3
- cpe:2.3:a:oracle:financial_services_liquidity_risk_management:8.0.5.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:weblogic_server:14.1.1.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_data_foundation:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.8
- cpe:2.3:a:oracle:healthcare_translational_research:3.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.58:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:fusion_middleware_mapviewer:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.55:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_data_foundation:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:agile_product_lifecycle_management_for_process:6.1:*:*:*:*:*:*:*

- cpe:2.3:a:oracle:retail_customer_management_and_segmentation_foundation:19.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:bi_publisher:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_gateway:15.2.18:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_operations_monitor:*:*:*:*:*:*:*:* versions from (including) 4.1; versions up to (including) 4.3
- cpe:2.3:a:oracle:siebel_ui_framework:20.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_translational_research:3.3.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_data_integration_hub:*:*:*:*:*:*:*:* versions from (including) 8.0.5; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:utilities_mobile_workforce_management:*:*:*:*:*:*:*:* versions from (including) 2.3.0.1; versions up to (including) 2.3.0.3
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_internal_ratings_based_approach:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_service_level_management:13.3.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_management:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:bi_publisher:5.5.0.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_unifier:16.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:siebel_mobile_applications:*:*:*:*:*:*:*:* versions up to (including) 19.8
- cpe:2.3:a:oracle:retail_back_office:14.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_unified_inventory_management:7.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.0
- cpe:2.3:a:oracle:banking_digital_experience:18.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_back_office:14.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_customer_management_and_segmentation_foundation:18.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_diameter_signaling_router:8.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_testing_suite:13.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_hedge_management_and_ifrs_valuations:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:agile_product_lifecycle_management_for_process:6.2.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_testing_suite:13.2.0.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:webcenter_sites:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_asset_liability_management:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_simphony:*:*:*:*:*:*:*:* versions from (including) 19.1.0; versions up to (including) 19.1.2
- cpe:2.3:a:oracle:hospitality_simphony:18.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_profitability_management:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:communications_session_report_manager:8.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_route_manager:8.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jdeveloper:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_operations_monitor:4.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:backdropcms:backdrop:*:*:*:*:*:*:*:* versions from (including) 1.12.0; versions up to (excluding) 1.12.6
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 19.12.0; versions up to (including) 19.12.4
- cpe:2.3:a:oracle:primavera_unifier:*:*:*:*:*:*:*:* versions from (including) 17.7; versions up to (including) 17.12
- cpe:2.3:a:oracle:storagetek_tape_analytics_sw_tool:2.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:diagnostic_assistant:2.12.36:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:11.2.0.4:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:insurance_performance_insight:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_price_creation_and_discovery:*:*:*:*:*:*:*:* versions from (including) 8.0.4; versions up to (including) 8.0.7
- cpe:2.3:a:oracle:retail_point-of-service:14.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 17.12.0; versions up to (including) 17.12.7
- cpe:2.3:a:oracle:banking_platform:*:*:*:*:*:*:*:* versions from (including) 2.4.0; versions up to (including) 2.10.0
- cpe:2.3:a:oracle:communications_billing_and_revenue_management:7.5:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_market_risk_measurement_and_management:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_insbridge_rating_and_underwriting:*:*:*:*:*:*:*:* versions from (including) 5.0.0.0; versions up to (including) 5.6.0.0
- cpe:2.3:a:oracle:jd_edwards_enterpriseone_tools:9.2:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:oncommand_system_manager:*:*:*:*:*:*:*:* versions from (including) 3.0; versions up to (including) 3.1.3
- cpe:2.3:a:oracle:jdeveloper_and_adf:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_diameter_signaling_router:8.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_measurement_and_management:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_market_risk_measurement_and_management:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_data_governance_for_us_regulatory_reporting:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.9
- cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:system_utilities:19.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_ifrs_17_analyzer:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_route_manager:8.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_returns_management:14.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_testing_suite:13.3.0.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:service_bus:11.1.1.9.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_central_office:14.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_foundation:7.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:agile_product_lifecycle_management_for_process:6.2.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jdeveloper_and_adf:11.1.1.9.0:*:*:*:*:*:*:*
- cpe:2.3:a:backdropcms:backdrop:*:*:*:*:*:*:*:* versions from (including) 1.11.0; versions up to (excluding) 1.11.9
- cpe:2.3:a:oracle:banking_digital_experience:19.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_basic:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_regulatory_reporting_for_european_banking_authority:8.0.7:*:*:*:*:*:*:*

CVE-2020-11022 suppress

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.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:

- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:

- CONFIRM - https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2
- CONFIRM - https://security.netapp.com/advisory/ntap-20200511-0006/
- CONFIRM - https://www.drupal.org/sa-core-2020-002
- CONFIRM - https://www.tenable.com/security/tns-2020-10
- CONFIRM - https://www.tenable.com/security/tns-2020-11
- CONFIRM - https://www.tenable.com/security/tns-2021-02
- DEBIAN - DSA-4693
- FEDORA - FEDORA-2020-0b32a59b54
- FEDORA - FEDORA-2020-11be4b36d4

- FEDORA - FEDORA-2020-36d2db5f51
- FEDORA - FEDORA-2020-fbb94073a1
- FEDORA - FEDORA-2020-fe94df8c34
- GENTOO - GLSA-202007-03
- MISC - http://packetstormsecurity.com/files/162159/jQuery-1.2-Cross-Site-Scripting.html
- MISC - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
- MISC - https://github.com/jquery/jquery/commit/1d61fd9407e6fbe82fe55cb0b938307aa0791f77
- MISC - https://jquery.com/upgrade-guide/3.5/
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [airflow-commits] 20200820 [GitHub] [airflow] breser opened a new issue #10429: jquery dependency needs to be updated to 3.5.0 or newer
- MLIST - [debian-lts-announce] 20210326 [SECURITY] [DLA 2608-1] jquery security update
- MLIST - [flink-dev] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20201129 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210209 [jira] [Comment Edited] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210209 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210422 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210422 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210429 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210429 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- SUSE - openSUSE-SU-2020:1060
- SUSE - openSUSE-SU-2020:1106
- SUSE - openSUSE-SU-2020:1888
- info - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:oracle:communications_billing_and_revenue_management:7.5.0.23.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_profitability_management:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_materials_control:18.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_funds_transfer_pricing:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_analytical_applications_reconciliation_framework:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_webrtc_session_controller:7.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation_for_mobile_devices:*:*:*:*:*:*:*:* versions from (including) 12.2.0; versions up to (including) 12.2.20
- cpe:2.3:a:oracle:policy_automation_connector_for_siebel:10.4.6:*:*:*:*:*:*:*
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 7.0; versions up to (excluding) 7.70
- cpe:2.3:a:oracle:financial_services_institutional_performance_analytics:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_price_creation_and_discovery:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_regulatory_reporting_for_european_banking_authority:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.1.0
- cpe:2.3:a:oracle:banking_digital_experience:18.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_institutional_performance_analytics:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_profitability_management:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_measurement_and_management:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_asset_liability_management:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_hedge_management_and_ifrs_valuations:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.8
- cpe:2.3:a:oracle:financial_services_asset_liability_management:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_allocation_manager_for_enterprise_profitability:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:policy_automation:*:*:*:*:*:*:*:* versions from (including) 12.2.0; versions up to (including) 12.2.20
- cpe:2.3:a:oracle:weblogic_server:14.1.1.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_profitability_management:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_accounting_analyzer:8.0.9:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.58:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:enterprise_session_border_controller:8.4:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_customer_management_and_segmentation_foundation:19.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_funds_transfer_pricing:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_application_session_controller:3.8m0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_basic:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.8
- cpe:2.3:a:oracle:financial_services_data_integration_hub:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:siebel_ui_framework:20.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_loan_loss_forecasting_and_provisioning:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.8
- cpe:2.3:a:oracle:financial_services_data_foundation:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.1.0
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 8.7.0; versions up to (excluding) 8.7.14
- cpe:2.3:a:oracle:financial_services_funds_transfer_pricing:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jdeveloper:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_billing_and_revenue_management:12.0.0.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_internal_ratings_based_approach:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_management:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_back_office:14.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_data_integration_hub:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.56:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jdeveloper:11.1.1.9.0:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:max_data:-:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_diameter_signaling_router_idih\::*:*:*:*:*:*:*:* versions from (including) 8.0.0; versions up to (including) 8.2.2
- cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:* versions from (including) 1.2; versions up to (excluding) 3.5.0
- cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:8.57:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_balance_sheet_planning:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_data_integration_hub:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_insbridge_rating_and_underwriting:5.6.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_digital_experience:18.3:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_back_office:14.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_measurement_and_management:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_hedge_management_and_ifrs_valuations:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_simphony:18.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_simphony:*:*:*:*:*:*:*:* versions from (including) 19.1.0; versions up to (including) 19.1.2
- cpe:2.3:a:oracle:financial_services_asset_liability_management:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_digital_experience:20.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:hospitality_simphony:18.2:*:*:*:*:*:*:*
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 8.8.0; versions up to (excluding) 8.8.6
- cpe:2.3:a:oracle:jdeveloper:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_foundation:7.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_institutional_performance_analytics:8.0.7:*:*:*:*:*:*:*

- cpe:2.3:a:oracle:financial_services_regulatory_reporting_for_us_federal_reserve:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.9
- cpe:2.3:a:oracle:enterprise_manager_ops_center:12.4.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_data_foundation:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.1.0
- cpe:2.3:a:oracle:insurance_insbridge_rating_and_underwriting:*:*:*:*:*:*:*:* versions from (including) 5.0.0.0; versions up to (including) 5.6.0.0
- cpe:2.3:a:oracle:financial_services_market_risk_measurement_and_management:8.0.6:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:oncommand_insight:-:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:agile_product_supplier_collaboration_for_process:6.2.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_price_creation_and_discovery:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_loan_loss_forecasting_and_provisioning:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_foundation:7.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:oncommand_system_manager:*:*:*:*:*:*:*:* versions from (including) 3.0; versions up to (including) 3.1.3
- cpe:2.3:a:oracle:banking_digital_experience:18.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_market_risk_measurement_and_management:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:insurance_allocation_manager_for_enterprise_profitability:8.0.8:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_liquidity_risk_measurement_and_management:8.0.7:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_data_governance_for_us_regulatory_reporting:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.9
- cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:snap_creator_framework:-:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_internal_ratings_based_approach:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.8
- cpe:2.3:a:oracle:healthcare_foundation:7.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_analytical_applications_reconciliation_framework:*:*:*:*:*:*:*:* versions from (including) 8.0.6; versions up to (including) 8.0.8
- cpe:2.3:a:oracle:retail_returns_management:14.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_testing_suite:13.3.0.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_analytical_applications_infrastructure:*:*:*:*:*:*:*:* versions from (including) 8.0.6.0.0; versions up to (including) 8.1.0.0.0
- cpe:2.3:a:oracle:healthcare_foundation:7.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:financial_services_basel_regulatory_capital_basic:8.1.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_digital_experience:19.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_digital_experience:19.2:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:snapcenter:-:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:retail_returns_management:14.0:*:*:*:*:*:*:*

CVE-2020-11023 suppress

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.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6
- CONFIRM - https://security.netapp.com/advisory/ntap-20200511-0006/
- CONFIRM - https://www.drupal.org/sa-core-2020-002
- CONFIRM - https://www.tenable.com/security/tns-2021-02
- DEBIAN - DSA-4693
- FEDORA - FEDORA-2020-0b32a59b54
- FEDORA - FEDORA-2020-36d2db5f51
- FEDORA - FEDORA-2020-fbb94073a1
- FEDORA - FEDORA-2020-fe94df8c34
- GENTOO - GLSA-202007-03
- MISC - http://packetstormsecurity.com/files/162160/jQuery-1.0.3-Cross-Site-Scripting.html
- MISC - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released
- MISC - https://jquery.com/upgrade-guide/3.5/
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20210326 [SECURITY] [DLA 2608-1] jquery security update
- MLIST - [felix-commits] 20201208 [felix-dev] branch master updated: FELIX-6366 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023 (#64)
- MLIST - [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
- MLIST - [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
- MLIST - [felix-dev] 20201208 [jira] [Assigned] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023
- MLIST - [felix-dev] 20201208 [jira] [Commented] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023
- MLIST - [felix-dev] 20201208 [jira] [Created] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023
- MLIST - [felix-dev] 20201208 [jira] [Updated] (FELIX-6366) 1.0.3 < jQuery <3.4.0 is vulnerable to CVE-2020-11023
- MLIST - [felix-dev] 20201208 [jira] [Updated] (FELIX-6366) 1.0.3 < jQuery <3.5.0 is vulnerable to CVE-2020-11023
- MLIST - [flink-dev] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20201105 [jira] [Created] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20201129 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210209 [jira] [Comment Edited] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210209 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210422 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210422 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210429 [jira] [Commented] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [flink-issues] 20210429 [jira] [Updated] (FLINK-20014) Resolve CVE-2020-11022 and CVE-2020-11023 in scala-compiler
- MLIST - [hive-commits] 20200915 [hive] branch master updated: HIVE-24039 : Update jquery version to mitigate CVE-2020-11023 (#1403)
- MLIST - [hive-dev] 20200813 [jira] [Created] (HIVE-24039) update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-gitbox] 20200813 [GitHub] [hive] rajkrrsingh opened a new pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-gitbox] 20200911 [GitHub] [hive] rajkrrsingh closed pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-gitbox] 20200911 [GitHub] [hive] rajkrrsingh opened a new pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-gitbox] 20200912 [GitHub] [hive] rajkrrsingh closed pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-gitbox] 20200912 [GitHub] [hive] rajkrrsingh opened a new pull request #1403: Hive 24039 : Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-gitbox] 20200915 [GitHub] [hive] kgyrtkirk merged pull request #1403: HIVE-24039 : Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200813 [jira] [Assigned] (HIVE-24039) update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200813 [jira] [Updated] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200902 [jira] [Assigned] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200902 [jira] [Comment Edited] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023

- MLIST - [hive-issues] 20200902 [jira] [Commented] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200902 [jira] [Work started] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200904 [jira] [Assigned] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200915 [jira] [Resolved] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200915 [jira] [Updated] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [hive-issues] 20200915 [jira] [Work logged] (HIVE-24039) Update jquery version to mitigate CVE-2020-11023
- MLIST - [nifi-commits] 20200930 svn commit: r1882168 - /nifi/site/trunk/security.html
- SUSE - openSUSE-SU-2020:1060
- SUSE - openSUSE-SU-2020:1106
- SUSE - openSUSE-SU-2020:1888
- info - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:oracle:jd_edwards_enterpriseone_tools:*:*:*:*:*:*:*:* versions up to (excluding) 9.2.5.0
- cpe:2.3:a:oracle:financial_services_regulatory_reporting_for_de_nederlandsche_bank:8.0.4:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:storagetek_tape_analytics_sw_tool:2.3.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:12.1.0.2:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_operations_monitor:3.4:*:*:*:*:*:*:*
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 7.0; versions up to (excluding) 7.70
- cpe:2.3:a:oracle:webcenter_sites:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:12.2.0.1:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:hyperion_financial_reporting:11.1.2.4:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_report_manager:8.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_report_manager:8.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 8.8.0; versions up to (excluding) 8.8.6
- cpe:2.3:a:oracle:communications_session_route_manager:8.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 19.12.0; versions up to (including) 19.12.4
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 16.2; versions up to (including) 16.2.11
- cpe:2.3:a:oracle:communications_element_manager:8.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_element_manager:8.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:18c:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:healthcare_translational_research:3.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_report_manager:8.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:rest_data_services:11.2.0.4:*:*:*:-:*:*:*
- cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:* versions from (including) 1.0.3; versions up to (excluding) 3.5.0
- cpe:2.3:a:oracle:communications_analytics:12.1.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_element_manager:8.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 17.12.0; versions up to (including) 17.12.7
- cpe:2.3:a:oracle:banking_platform:*:*:*:*:*:*:*:* versions from (including) 2.4.0; versions up to (including) 2.10.0
- cpe:2.3:a:oracle:weblogic_server:14.1.1.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:healthcare_translational_research:3.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:siebel_mobile:*:*:*:*:*:*:*:* versions up to (including) 20.12
- cpe:2.3:a:oracle:communications_session_route_manager:8.2.0:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:oncommand_insight:-:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:snapcenter_server:-:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:jd_edwards_enterpriseone_orchestrator:*:*:*:*:*:*:*:* versions up to (excluding) 9.2.5.0
- cpe:2.3:a:netapp:oncommand_system_manager:*:*:*:*:*:*:*:* versions from (including) 3.0; versions up to (including) 3.1.3
- cpe:2.3:a:oracle:communications_operations_monitor:*:*:*:*:*:*:*:* versions from (including) 4.1; versions up to (including) 4.3
- cpe:2.3:a:oracle:peoplesoft_enterprise_human_capital_management_resources:9.2:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:snap_creator_framework:-:*:*:*:*:*:*:*
- cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:* versions from (including) 8.7.0; versions up to (excluding) 8.7.14
- cpe:2.3:a:oracle:rest_data_services:19c:*:*:*:-:*:*:*
- cpe:2.3:a:oracle:healthcare_translational_research:3.3.2:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:communications_session_route_manager:8.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_express:*:*:*:*:*:*:*:* versions up to (excluding) 20.2
- cpe:2.3:a:oracle:healthcare_translational_research:3.3.1:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:primavera_gateway:*:*:*:*:*:*:*:* versions from (including) 18.8.0; versions up to (including) 18.8.9
- cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:application_testing_suite:13.3.0.1:*:*:*:*:*:*:*
- cpe:2.3:a:netapp:max_data:-:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:webcenter_sites:12.2.1.4.0:*:*:*:*:*:*:*
- cpe:2.3:a:oracle:banking_enterprise_collections:*:*:*:*:*:*:*:* versions from (including) 2.7.0; versions up to (including) 2.8.0
- cpe:2.3:a:oracle:communications_interactive_session_recorder:*:*:*:*:*:*:*:* versions from (including) 6.1; versions up to (including) 6.4

FusionRegistry.war: bootstrap.min.js

File Path: F:\tomcats\apache-tomcat-9.0.44\webapps\FusionRegistry.war\assets\matrix\js\vendor\bootstrap.min.js
MD5: 4becdc9104623e891fbb9d38bba01be4
SHA1: 6c264e0e0026ab5ece49350c6a8812398e696cbb
SHA256:4a4de7903ea62d330e17410ea4db6c22bcbeb350ac6aa402d6b54b4c0cbed327

Evidence

Identifiers

- pkg:javascript/bootstrap@3.3.5 (*Confidence*:Highest)

Published Vulnerabilities

CVE-2018-14040 suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/
- MISC - https://github.com/twbs/bootstrap/issues/26423
- MISC - https://github.com/twbs/bootstrap/issues/26625
- MISC - https://github.com/twbs/bootstrap/pull/26630
- MLIST - [debian-lts-announce] 20180827 [SECURITY] [DLA 1479-1] twitter-bootstrap3 security update
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- info - https://github.com/twbs/bootstrap/issues/20184

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.0.0; versions up to (excluding) 4.1.2
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.0
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*

CVE-2018-14041 suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/
- MISC - https://github.com/twbs/bootstrap/issues/26423
- MISC - https://github.com/twbs/bootstrap/issues/26627
- MISC - https://github.com/twbs/bootstrap/pull/26630
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- REDHAT - RHSA-2019:1456
- info - https://github.com/twbs/bootstrap/issues/20184

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.0.0; versions up to (excluding) 4.1.2
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*

CVE-2018-14042 suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/
- MISC - https://github.com/twbs/bootstrap/issues/26423
- MISC - https://github.com/twbs/bootstrap/issues/26628
- MISC - https://github.com/twbs/bootstrap/pull/26630
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- info - https://github.com/twbs/bootstrap/issues/20184

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.0.0; versions up to (excluding) 4.1.2
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.0
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*

CVE-2019-8331 suppress

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.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BID - 107375
- BUGTRAQ - 20190509 dotCMS v5.1.1 Vulnerabilities
- CONFIRM - https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/
- CONFIRM - https://support.f5.com/csp/article/K24383845
- CONFIRM - https://support.f5.com/csp/article/K24383845?utm_source=f5support&utm_medium=RSS
- FULLDISC - 20190510 Re: dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 HTML Injection & XSS Vulnerability
- FULLDISC - 20190510 dotCMS v5.1.1 Vulnerabilities
- MISC - http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- MISC - https://github.com/twbs/bootstrap/pull/28236
- MISC - https://github.com/twbs/bootstrap/releases/tag/v3.4.1
- MISC - https://github.com/twbs/bootstrap/releases/tag/v4.3.1
- MLIST - [drill-dev] 20191017 Dependencies used by Drill contain known vulnerabilities
- MLIST - [drill-dev] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [drill-issues] 20191021 [jira] [Created] (DRILL-7416) Updates required to dependencies to resolve potential security vulnerabilities
- MLIST - [flink-dev] 20190811 Apache flink 1.7.2 security issues
- MLIST - [flink-user] 20190811 Apache flink 1.7.2 security issues
- MLIST - [flink-user] 20190813 Apache flink 1.7.2 security issues
- MLIST - [flink-user] 20190813 Re: Apache flink 1.7.2 security issues
- MLIST - [hbase-issues] 20201116 [GitHub] [hbase] symat opened a new pull request #2661: HBASE-25261 Upgrade Bootstrap to 3.4.1
- MLIST - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- MLIST - [superset-dev] 20190926 Re: [VOTE] Release Superset 0.34.1 based on Superset 0.34.1rc1
- REDHAT - RHSA-2019:1456
- REDHAT - RHSA-2019:3023
- REDHAT - RHSA-2019:3024
- info - https://github.com/twbs/bootstrap/issues/28236

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5

- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions from (including) 4.3.0; versions up to (excluding) 4.3.1
- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:redhat:virtualization_manager:4.3:*:*:*:*:*:*:*
- cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* versions up to (excluding) 3.4.1
- cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_edge_gateway:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5

FusionRegistry.war: commons-io-2.6.jar

Description:

The Apache Commons IO library contains utility classes, stream implementations, file filters,
file comparators, endian transformation classes, and much more.

License:

https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: F:\tomcats\apache-tomcat-9.0.44\webapps\FusionRegistry.war\WEB-INF\lib\commons-io-2.6.jar
MD5: 467c2a1f64319c99b5faf03fc78572af
SHA1: 815893df5f31da2ece4040fe0a12fd44b577afaf
SHA256:f877d304660ac2a142f3865badfc971dec7ed73c747c7f8d5d2f5139ca736513

Evidence

Identifiers

- pkg:maven/commons-io/commons-io@2.6 (*Confidence*:High)
- cpe:2.3:a:apache:commons_io:2.6:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2021-29425 suppress

In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\\..\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://issues.apache.org/jira/browse/IO-556
- MISC - https://lists.apache.org/thread.html/rc359823b5500e9a9a2572678ddb8e01d3505a7ffcadfa8d13b8780ab%40%3Cuser.commons.apache.org%3E
- MLIST - [commons-dev] 20210414 Re: [all] OSS Fuzz
- MLIST - [commons-dev] 20210415 Re: [all] OSS Fuzz
- MLIST - [creadur-dev] 20210427 [jira] [Closed] (RAT-281) Update commons-io to fix CVE-2021-29425 Moderate severity
- MLIST - [creadur-dev] 20210427 [jira] [Commented] (RAT-281) Update commons-io to fix CVE-2021-29425 Moderate severity
- MLIST - [creadur-dev] 20210427 [jira] [Created] (RAT-281) Update commons-io to fix CVE-2021-29425 Moderate severity
- MLIST - [creadur-dev] 20210427 [jira] [Updated] (RAT-281) Update commons-io to fix CVE-2021-29425 Moderate severity
- MLIST - [myfaces-dev] 20210504 [GitHub] [myfaces-tobago] lofwyr14 opened a new pull request #808: build: CVE fix
- MLIST - [pulsar-commits] 20210420 [GitHub] [pulsar] lhotari opened a new pull request #10287: [Security] Upgrade commons-io to address CVE-2021-29425
- MLIST - [pulsar-commits] 20210420 [GitHub] [pulsar] merlimat merged pull request #10287: [Security] Upgrade commons-io to address CVE-2021-29425
- MLIST - [pulsar-commits] 20210429 [pulsar] branch branch-2.7 updated: [Security] Upgrade commons-io to address CVE-2021-29425 (#10287)

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:commons_io:2.6:-:*:*:*:*:*:*
- ...

FusionRegistry.war: spring-rabbit-2.3.6.jar

Description:

Spring RabbitMQ Support

License:

Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0.txt

File Path: F:\tomcats\apache-tomcat-9.0.44\webapps\FusionRegistry.war\WEB-INF\lib\spring-rabbit-2.3.6.jar
MD5: 347f6f63ef08c99118a989360f14a4fc
SHA1: 52f23ba8dc15bb5c661f7825c207c47733a8dae6
SHA256:17a989b55046947244eae4238b804b2a0e2de693e7654d14d7bca569f82bd087

Evidence

Identifiers

- pkg:maven/org.springframework.amqp/spring-rabbit@2.3.6 (*Confidence*:High)
- cpe:2.3:a:pivotal_software:rabbitmq:2.3.6:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2014-9494 suppress

RabbitMQ before 3.4.0 allows remote attackers to bypass the loopback_users restriction via a crafted X-Forwareded-For header.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:
- CONFIRM - http://www.rabbitmq.com/release-notes/README-3.4.0.txt
- CONFIRM - https://groups.google.com/forum/#!topic/rabbitmq-users/DMkypbSvIyM
- MLIST - [oss-security] 20150103 Re: CVE request: insufficient 'X-Forwarded-For' header validation in rabbitmq-server
- XF - rabbitmq-cve20149494-sec-bypass(99685)

Vulnerable Software & Versions:

- cpe:2.3:a:pivotal_software:rabbitmq:*:*:*:*:*:*:*:* versions up to (including) 3.3.5

CVE-2018-11087 suppress

Pivotal Spring AMQP, 1.x versions prior to 1.7.10 and 2.x versions prior to 2.0.6, expose a man-in-the-middle vulnerability due to lack of hostname validation. A malicious user that has the ability to intercept traffic would be able to view data in transit.

CWE-295 Improper Certificate Validation

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://pivotal.io/security/cve-2018-11087

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:pivotal_software:rabbitmq:*:*:*:*:*:*:*:* versions up to (excluding) 4.8.0
- ...

CVE-2018-1279 suppress

Pivotal RabbitMQ for PCF, all versions, uses a deterministically generated cookie that is shared between all machines when configured in a multi-tenant cluster. A remote attacker who can gain information about the network topology can guess this cookie and, if they have access to the right ports on any server in the MQ cluster can use this cookie to gain full control over the entire cluster.

CWE-330 Use of Insufficiently Random Values

CVSSv2:
- Base Score: LOW (3.3)
- Vector: /AV:A/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://pivotal.io/security/cve-2018-1279

Vulnerable Software & Versions:

- cpe:2.3:a:pivotal_software:rabbitmq:*:*:*:*:*:pivotal_cloud_foundry:*:*

CVE-2019-11281 suppress

Pivotal RabbitMQ, versions prior to v3.7.18, and RabbitMQ for PCF, versions 1.15.x prior to 1.15.13, versions 1.16.x prior to 1.16.6, and versions 1.17.x prior to 1.17.3, contain two components, the virtual host limits page, and the federation management UI, which do not properly sanitize user input. A remote authenticated malicious user with administrative access could craft a cross site scripting attack that would gain access to virtual hosts and policy management information.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://pivotal.io/security/cve-2019-11281
- FEDORA - FEDORA-2019-6497f51791
- FEDORA - FEDORA-2019-74d2feb5be
- REDHAT - RHSA-2020:0078

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:pivotal_software:rabbitmq:*:*:*:*:*:*:*:* versions up to (excluding) 3.7.18
- ...

CVE-2020-5419 suppress

RabbitMQ versions 3.8.x prior to 3.8.7 are prone to a Windows-specific binary planting security vulnerability that allows for arbitrary code execution. An attacker with write privileges to the RabbitMQ installation directory and local access on Windows could carry out a local binary hijacking (planting) attack and execute arbitrary code.

CWE-427 Uncontrolled Search Path Element

CVSSv2:
- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: MEDIUM (6.7)
- Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://tanzu.vmware.com/security/cve-2020-5419

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:pivotal_software:rabbitmq:*:*:*:*:*:*:*:* versions up to (excluding) 3.7.28
- ...

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the NPM Public Advisories.
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype OSS Index.