Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

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*: Thu, 13 May 2021 12:23:54 +0100
- *Dependencies Scanned*: 788 (751 unique)
- *Vulnerable Dependencies*: 1
- *Vulnerabilities Found*: 4
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
FusionMetadataRegistry-10.7.0.war: bootstrap.min.js		pkg:javascript/bootstrap@3.3.5	MEDIUM	4		3

Dependencies

FusionMetadataRegistry-10.7.0.war: bootstrap.min.js

File Path: F:\git\Git2\fusion-webapp-metadataregistry\target\FusionMetadataRegistry-10.7.0.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 up to (excluding) 3.4.0
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- 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:beta3:*:*:*:*:*:*
- 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:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*

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:alpha6:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta2:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:beta3:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha5:*:*:*:*:*:*
- 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:alpha4:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha:*:*:*:*:*:*
- cpe:2.3:a:getbootstrap:bootstrap:4.0.0:alpha2:*:*:*:*:*:*

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

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:redhat:virtualization_manager:4.3:*:*:*:*:*:*:*
- 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) 12.1.0; versions up to (excluding) 12.1.5.1
- 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_analytics:*:*:*:*:*:*:*:* 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_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) 14.0.0; versions up to (excluding) 14.1.2.5
- 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_local_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- 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_global_traffic_manager:*:*:*:*:*:*:*:* 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) 15.0.0; versions up to (excluding) 15.1.0
- 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_webaccelerator:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- 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_analytics:*:*:*:*:*:*:*:* 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_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_domain_name_system:*:*:*:*:*:*:*:* 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_webaccelerator:*:*:*:*:*:*:*:* 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_global_traffic_manager:*:*:*:*:*:*:*:* versions from (including) 14.0.0; versions up to (excluding) 14.1.2.5
- 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_edge_gateway:*:*:*:*:*:*:*:* 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) 14.0.0; versions up to (excluding) 14.1.2.5
- 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_policy_enforcement_manager:*:*:*:*:*:*:*:* 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) 12.1.0; versions up to (excluding) 12.1.5.1
- 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_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_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 15.0.0; versions up to (excluding) 15.1.0
- cpe:2.3:a:f5:big-ip_policy_enforcement_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_fraud_protection_service:*:*:*:*:*:*:*:* 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) 13.0.0; versions up to (excluding) 13.1.3.4
- 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) 14.0.0; versions up to (excluding) 14.1.2.5
- 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_link_controller:*:*:*:*:*:*:*:* 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) 13.0.0; versions up to (excluding) 13.1.3.4
- 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_link_controller:*:*:*:*:*:*:*:* versions from (including) 12.1.0; versions up to (excluding) 12.1.5.1
- 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_access_policy_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4
- 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_application_security_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_global_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) 13.0.0; versions up to (excluding) 13.1.3.4
- 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_application_acceleration_manager:*:*:*:*:*:*:*:* versions from (including) 13.0.0; versions up to (excluding) 13.1.3.4

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.