



CVE-2018-12541

Published on: 10/10/2018 12:00:00 AM UTC

Last Modified on: 04/19/2022 04:13:00 PM UTC

CVE-2018-12541

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Vert.x](#) from [Eclipse](#) contain the following vulnerability:

In version from 3.0.0 to 3.5.3 of Eclipse Vert.x, the WebSocket HTTP upgrade implementation buffers the full http request before doing the handshake, holding the entire request body in memory. There should be a reasonable limit (8192 bytes) above which the WebSocket gets an HTTP response with the 413 status code and the connection gets

closed.

CVE-2018-12541 has been assigned by security@eclipse.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **The Eclipse Foundation - Eclipse Vert.x** version **>= 3.0**

Affected Vendor/Software: **The Eclipse Foundation - Eclipse Vert.x** version **<= 3.5.3**

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	 MLIST [pulsar-commits] 20210419 [pulsar] branch master updated: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541 (#10261)
539170 – (CVE-2018-12541) WebSocket HTTP upgrade implementation buffers the full http request before doing the handshake	Third Party Advisory bugs.eclipse.org text/html	 CONFIRM bugs.eclipse.org/bugs/show_bug.cgi?id=539170
Pony Mail!	lists.apache.org text/html	 MLIST [pulsar-commits] 20210419 [GitHub] [pulsar] eolivelli merged pull request #10261: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2018:2946
Pony Mail!	lists.apache.org text/html	 MLIST [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
Pony Mail!	lists.apache.org text/html	 MLIST [pulsar-commits] 20210419 [GitHub] [pulsar] lhotari opened a new pull request #10261: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541
Pony Mail!	lists.apache.org text/html	 MLIST [pulsar-commits] 20210419 [GitHub] [pulsar] lhotari edited a comment on pull request #10261: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541
WebSocket upgrade request body limit · Issue #2648 · eclipse-vertx/vert.x · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/eclipse-vertx/vert.x/issues/2648
Pony Mail!	lists.apache.org text/html	 MLIST [bookkeeper-issues] 20210507 [GitHub] [bookkeeper] dlg99 commented on pull request #2693: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541
Pony Mail!	lists.apache.org text/html	 MLIST [pulsar-commits] 20210419 [GitHub] [pulsar] lhotari commented on pull request #10261: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541
Pony Mail!	lists.apache.org text/html	 MLIST [pulsar-commits] 20210513 [pulsar] 30/46: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541 (#10261)
Pony Mail!	lists.apache.org text/html	 MLIST [bookkeeper-commits] 20210817 [bookkeeper] 01/03: [Security] Upgrade vertx to 3.9.8, addresses CVE-2018-12541 (#2693)
Pony Mail!	lists.apache.org text/html	 MLIST [bookkeeper-issues] 20210618 [GitHub] [bookkeeper] lhotari commented on pull request #2693: [Security] Upgrade vertx to 3.9.8, addresses CVE-2018-12541
Pony Mail!	lists.apache.org text/html	 MLIST [bookkeeper-issues] 20210623 [GitHub] [bookkeeper] sijie merged pull request #2693: [Security] Upgrade vertx to 3.9.8, addresses CVE-2018-12541
Pony Mail!	lists.apache.org text/html	 MLIST [bookkeeper-issues] 20210419 [GitHub] [bookkeeper] lhotari opened a new pull request #2693: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-12541
Pony Mail!	lists.apache.org text/html	 MLIST [bookkeeper-issues] 20210421 [GitHub] [bookkeeper] lhotari commented on pull request #2693: [Security] Upgrade vertx to 3.9.7, addresses CVE-2018-

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[981498](#) Java (maven) Security Update for io.vertx:vertx-core (GHSA-45xm-v8gq-7jqx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eclipse	Vert.x	All	All	All	All
Application	Eclipse	Vert.x	All	All	All	All

`cpe:2.3:a:eclipse:vert.x:*:*:*:*:*:*:`

`cpe:2.3:a:eclipse:vert.x:*:*:*:*:*:*:`

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)