



# CVE-2019-17640

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

## Summary

<b>CVE</b>	CVE-2019-17640
<b>State</b>	PUBLIC
<b>Assigner</b>	security@eclipse.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-10-15 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:06:00 UTC
<b>Description</b>	In Eclipse Vert.x 3.4.x up to 3.9.4, 4.0.0.milestone1, 4.0.0.milestone2, 4.0.0.milestone3, 4.0.0.milestone4, 4.0.0.milestone5,

## Risk And Classification

**Problem Types:** CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eclipse	Vert.x	4.0.0	beta1	All	All
Application	Eclipse	Vert.x	4.0.0	beta2	All	All
Application	Eclipse	Vert.x	4.0.0	beta3	All	All
Application	Eclipse	Vert.x	4.0.0	milestone1	All	All
Application	Eclipse	Vert.x	4.0.0	milestone2	All	All
Application	Eclipse	Vert.x	4.0.0	milestone3	All	All
Application	Eclipse	Vert.x	4.0.0	milestone4	All	All
Application	Eclipse	Vert.x	4.0.0	milestone5	All	All
Application	Eclipse	Vert.x	4.0.0	beta1	All	All
Application	Eclipse	Vert.x	4.0.0	beta2	All	All
Application	Eclipse	Vert.x	4.0.0	beta3	All	All
Application	Eclipse	Vert.x	4.0.0	milestone1	All	All
Application	Eclipse	Vert.x	4.0.0	milestone2	All	All
Application	Eclipse	Vert.x	4.0.0	milestone3	All	All
Application	Eclipse	Vert.x	4.0.0	milestone4	All	All
Application	Eclipse	Vert.x	4.0.0	milestone5	All	All
Application	Eclipse	Vert.x	All	All	All	All

References				
Reference	Source	Link	Tags	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
567416 – (CVE-2019-17640) Eclipse Vert.x StaticHandler doesn't correctly process back slashes	CONFIRM	<a href="https://bugs.eclipse.org">bugs.eclipse.org</a>	Vendor A	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MISC	<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical	
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical	

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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

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

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)