CVE-2019-17640

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-17640
State	PUBLIC
Assigner	security@eclipse.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-15 21:15:00 UTC
Updated	2023-11-07 03:06:00 UTC
Description	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	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
567416 – (CVE-2019-17640) Eclipse Vert.x StaticHandler doesn't correctly process back slashes	CONFIRM	bugs.eclipse.org	Vendor A
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MISC	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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