



CVE-2022-0552

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

Summary

CVE	CVE-2022-0552
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-11 20:15:00 UTC
Updated	2023-02-12 22:15:00 UTC
Description	A flaw was found in the original fix for the netty-codec-http CVE-2021-21409, where the OpenShift Logging openshift-logging

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Origin-aggregated-logging	3.11	All	All	All

References

Reference
Red Hat Customer Portal - Access to 24x7 support and knowledge
2052539 – (CVE-2022-0552) CVE-2022-0552 origin-aggregated-logging/elasticsearch: Incomplete fix for netty-codec-http CVE-2021-21409
Update netty to 4.1.63 · openshift/origin-aggregated-logging@d6b72d6 · GitHub
Red Hat Customer Portal - Access to 24x7 support and knowledge
Red Hat Customer Portal - Access to 24x7 support and knowledge
Red Hat Customer Portal - Access to 24x7 support and knowledge
Red Hat Customer Portal - Access to 24x7 support and knowledge
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

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