



CVE-2023-31418

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

Summary

CVE	CVE-2023-31418
State	PUBLIC
Assigner	security@elastic.co
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-26 18:15:00 UTC
Updated	2023-11-30 22:15:00 UTC
Description	An issue has been identified with how Elasticsearch handled incoming requests on the HTTP layer. An unauthenticated user

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elastic	Elasticsearch	All	All	All	All
Application	Elastic	Elasticsearch	All	All	All	All
Application	Elastic	Elastic Cloud Enterprise	3.6.0	All	All	All
Application	Elastic	Elastic Cloud Enterprise	All	All	All	All

References

Reference	Source	Link	Tag
security.netapp.com/advisory/ntap-20231130-0005		security.netapp.com	
www.elastic.co/community/security	MISC	www.elastic.co	
Elasticsearch 8.9.0, 7.17.13 Security Update - Security Announcements - Discuss the Elastic Stack	MISC	discuss.elastic.co	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995771](#) Java (Maven) Security Update for org.elasticsearch:elasticsearch (GHSA-2cqf-6xv9-f22w)

© [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](#)