



CVE-2022-29078

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

Summary

CVE	CVE-2022-29078
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-25 15:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	The ejs (aka Embedded JavaScript templates) package 3.1.6 for Node.js allows server-side template injection in settings[vi

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ejs	Ejs	3.1.6	All	All	All

References

Reference	Source	Link	Tags
EJS, Server side template injection RCE (CVE-2022-29078) - writeup ~#whoami <Eslam Salem>	MISC	eslam.io	
Releases · mde/ejs · GitHub	MISC	github.com	
CVE-2022-29078 Node.js Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canceled
NVD vulnerability detail	NVD	nvd.nist.gov	canceled

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180820](#) Debian Security Update for node-ejs (CVE-2022-29078)

[905138](#) Common Base Linux Mariner (CBL-Mariner) Security Update for prometheus (12608)

© [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](#)