



CVE-2020-7699

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

Summary

CVE	CVE-2020-7699
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-30 09:15:00 UTC
Updated	2022-12-02 19:56:00 UTC
Description	This affects the package express-fileupload before 1.1.8. If the parseNested option is enabled, sending a corrupt HTTP req

Risk And Classification

Problem Types: CWE-1321

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Express-fileupload Project	Express-fileupload	All	All	All	All
Application	Express-fileupload Project	Express-fileupload	All	All	All	All
Application	Netapp	Max Data	-	All	All	All

References

Reference	Source	Link	Tags
Prototype Pollution in express-fileupload Snyk	CONFIRM	snyk.io	Exploit, Third Party
Prototype Pollution · Issue #236 · richardgirges/express-fileupload · GitHub	CONFIRM	github.com	Exploit, Third Party
CVE-2020-7699 Nodejs Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: po6ix

Legacy QID Mappings

© [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](#)