



CVE-2023-43654

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

Summary

CVE	CVE-2023-43654
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-28 23:15:00 UTC
Updated	2023-10-31 18:35:00 UTC
Description	TorchServe is a tool for serving and scaling PyTorch models in production. TorchServe default configuration lacks proper in

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pytorch	Torchserve	All	All	All	All

References

Reference	Source	L
PyTorch Model Server Registration / Deserialization Remote Code Execution ~ Packet Storm	MISC	p
Release TorchServe v0.8.2 Release Notes · pytorch/serve · GitHub	MISC	g
TorchServe SSRF · Advisory · pytorch/serve · GitHub	MISC	g
Issue warning about allowed_urls when default value is used by namannandan · Pull Request #2534 · pytorch/serve · GitHub	MISC	g
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995497](#) Python (Pip) Security Update for torchserve (GHSA-8fxr-qfr9-p34w)

© [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](#)