



CVE-2022-40468

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-40468
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-19 17:15:00 UTC
Updated	2023-05-21 22:15:00 UTC
Description	Potential leak of left-over heap data if custom error page templates containing special non-standard variables are used. Tin

Risk And Classification

Problem Types: CWE-1188

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tinyproxy Project	Tinyproxy	All	All	All	All
Application	Tinyproxy Project	Tinyproxy	All	All	All	All

References

Reference	Source
Potential runtime system sensitive information disclosure through special HTTP requests. · Issue #457 · tinyproxy/tinyproxy · GitHub	MISC
tinyproxy/reqs.c at 84f203fb1c4733608c7283bbe794005a469c4b00 · tinyproxy/tinyproxy · GitHub	MISC
Tinyproxy: Memory Disclosure (GLSA 202305-27) — Gentoo security	GENTOO
GitHub - tinyproxy/tinyproxy: tinyproxy - a light-weight HTTP/HTTPS proxy daemon for POSIX operating systems	MISC
Potential runtime system sensitive information disclosure through special HTTP requests. · Issue #457 · tinyproxy/tinyproxy · GitHub	MISC
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[184192](#) Debian Security Update for tinyproxy (CVE-2022-40468)

502606 Alpine Linux Security Update for tinyproxy

504476 Alpine Linux Security Update for tinyproxy

710730 Gentoo Linux Tinyproxy Memory Disclosure Vulnerability (GLSA 202305-27)

© [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](#)