



CVE-2017-5963

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

Summary

CVE	CVE-2017-5963
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-12 04:59:00 UTC
Updated	2019-03-08 19:50:00 UTC
Description	An issue was discovered in caddy (for TYPO3) before 7.2.10. The vulnerability exists due to insufficient filtration of user-sup

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Caddy Project	Caddy	2.1.4	alpha	All	All
Application	Caddy Project	Caddy	2.1.5	alpha	All	All
Application	Caddy Project	Caddy	2.1.6	alpha	All	All
Application	Caddy Project	Caddy	3.0.0	alpha	All	All
Application	Caddy Project	Caddy	4.0.0	alpha	All	All
Application	Caddy Project	Caddy	4.0.1	alpha	All	All
Application	Caddy Project	Caddy	4.0.12	alpha	All	All
Application	Caddy Project	Caddy	4.0.2	alpha	All	All
Application	Caddy Project	Caddy	4.0.3	alpha	All	All
Application	Caddy Project	Caddy	6.0.1	alpha	All	All
Application	Caddy Project	Caddy	6.0.12	beta	All	All
Application	Caddy Project	Caddy	6.0.14	beta	All	All
Application	Caddy Project	Caddy	6.0.2	alpha	All	All
Application	Caddy Project	Caddy	6.0.9	alpha	All	All
Application	Caddy Project	Caddy	6.1.0	beta	All	All
Application	Caddy Project	Caddy	6.2.1	beta	All	All
Application	Caddy Project	Caddy	6.3.0	beta	All	All

Application	Caddy Project	Caddy	6.3.1	beta	All	All
Application	Caddy Project	Caddy	6.3.3	beta	All	All
Application	Caddy Project	Caddy	7.0.0	beta	All	All
Application	Caddy Project	Caddy	7.1.0	beta	All	All
Application	Caddy Project	Caddy	7.2.7	beta	All	All
Application	Caddy Project	Caddy	2.1.4	alpha	All	All
Application	Caddy Project	Caddy	2.1.5	alpha	All	All
Application	Caddy Project	Caddy	2.1.6	alpha	All	All
Application	Caddy Project	Caddy	3.0.0	alpha	All	All
Application	Caddy Project	Caddy	4.0.0	alpha	All	All
Application	Caddy Project	Caddy	4.0.1	alpha	All	All
Application	Caddy Project	Caddy	4.0.12	alpha	All	All
Application	Caddy Project	Caddy	4.0.2	alpha	All	All
Application	Caddy Project	Caddy	4.0.3	alpha	All	All
Application	Caddy Project	Caddy	6.0.1	alpha	All	All
Application	Caddy Project	Caddy	6.0.12	beta	All	All
Application	Caddy Project	Caddy	6.0.14	beta	All	All
Application	Caddy Project	Caddy	6.0.2	alpha	All	All
Application	Caddy Project	Caddy	6.0.9	alpha	All	All
Application	Caddy Project	Caddy	6.1.0	beta	All	All
Application	Caddy Project	Caddy	6.2.1	beta	All	All
Application	Caddy Project	Caddy	6.3.0	beta	All	All
Application	Caddy Project	Caddy	6.3.1	beta	All	All
Application	Caddy Project	Caddy	6.3.3	beta	All	All
Application	Caddy Project	Caddy	7.0.0	beta	All	All
Application	Caddy Project	Caddy	7.1.0	beta	All	All
Application	Caddy Project	Caddy	7.2.7	beta	All	All

References						
Reference					Source	Link
Bug #79325: TYPO3 EXTENTION 'caddy' - Cross-Site Scripting (XSS) - Caddy - TYPO3 Shopping Cart - TYPO3 Forge					MISC	forge.ty
TYPO3 Caddy Extension 'paymill/api/php/payment.php' Cross Site Scripting Vulnerability					BID	www.b
CVE Program record					CVE.ORG	www.c
NVD vulnerability detail					NVD	nvd.ni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)