



CVE-2018-19148

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

Summary

CVE	CVE-2018-19148
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-10 19:29:00 UTC
Updated	2019-01-30 18:09:00 UTC
Description	Caddy through 0.11.0 sends incorrect certificates for certain invalid requests, making it easier for attackers to enumerate ho

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Caddyserver	Caddy	All	All	All	All

References

Reference	Source	Link
tls: Restructure and improve certificate management by mholt · Pull Request #2015 · caddyserver/caddy · GitHub	MISC	github.com
Caddy serves wrong SSL cert for site that is not served on HTTPS port · Issue #1303 · mholt/caddy · GitHub	MISC	github.com
Making the Web a Better Place: Fixing Caddy Web Server Hostname Enumeration Vulnerability (CVE-2018-19148)	MISC	securitytra
Problem with the way Caddy serves multiple certificates · Issue #2334 · caddyserver/caddy · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)