



CVE-2012-6077

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

Summary

CVE	CVE-2012-6077
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-22 19:15:00 UTC
Updated	2023-05-26 17:46:00 UTC
Description	W3 Total Cache before 0.9.2.5 allows remote attackers to retrieve password hash information due to insecure storage of da

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Boldgrid	W3 Total Cache	All	All	All	All
Application	W3-edge	Total Cache	All	All	All	All
Application	W3-edge	Total Cache	All	All	All	All

References

Reference	Source	Link	Tags
WordPress W3 Total Cache plugin predictable cache filenames - Vulnerabilities - Acunetix	MISC	www.acunetix.com	Third P
cpai-24-oct2 Check Point Software	MISC	www.checkpoint.com	Third P
CVE-2012-6077	MISC	security-tracker.debian.org	Third P
oss-security - Re: CVE Request: W3 Total Cache - public cache exposure	MISC	www.openwall.com	Mailing
Security & W3 Total Cache 0.9.2.4	CONFIRM	www.w3-edge.com	Releas
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

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](#).

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