



CVE-2014-3946

Published on: 06/03/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

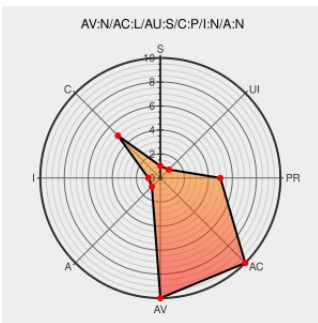
CVE-2014-3946

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Typo3](#) from [Typo3](#) contain the following vulnerability:

The query caching functionality in the Extbase Framework component in TYPO3 6.2.0 before 6.2.3 does not properly validate group permissions, which allows remote authenticated users to read arbitrary queries via unspecified vectors.

CVE-2014-3946 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

LOW

Authentication

SINGLE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

NONE

**Availability
Impact**

NONE

CVE References

Description

Tags

Link

Multiple Vulnerabilities in TYPO3 CMS - - TYPO3 - The Enterprise Open Source CMS

[Vendor Advisory](#)
[typo3.org](#)
[text/html](#)

[CONFIRM typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2014-001/](#)

Debian -- Security Information -- DSA-2942-1 typo3-src

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-2942](#)

oss-security - Re: CVE ID request: typo3

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20140603 Re: CVE ID request: typo3](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

994899 PHP (Composer) Security Update for typo3/cms (GHSA-vccp-5v5h-p8m6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Typo3	6.2	All	All	All
Application	Typo3	Typo3	6.2.0	beta1	All	All
Application	Typo3	Typo3	6.2.0	beta2	All	All
Application	Typo3	Typo3	6.2.0	beta3	All	All
Application	Typo3	Typo3	6.2.1	All	All	All
Application	Typo3	Typo3	6.2.2	All	All	All
Application	Typo3	Typo3	6.2	All	All	All
Application	Typo3	Typo3	6.2.0	beta1	All	All
Application	Typo3	Typo3	6.2.0	beta2	All	All
Application	Typo3	Typo3	6.2.0	beta3	All	All
Application	Typo3	Typo3	6.2.1	All	All	All
Application	Typo3	Typo3	6.2.2	All	All	All
cpe:2.3:a:typo3:typo3:6.2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:beta1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:beta2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:beta3:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:beta1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:beta2:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.0:beta3:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.1:*:*:*:*:*:						
cpe:2.3:a:typo3:typo3:6.2.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#)