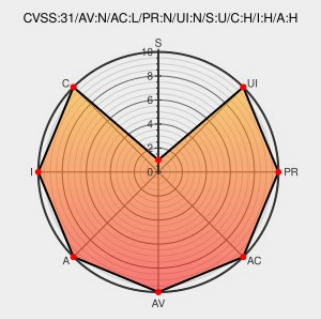
CVE-2011-3584

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:13 PM UTC

CVE-2011-3584

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wec Discussion Forum from Guidestar contain the following vulnerability:

The TYPO3 Core wec_discussion extension before 2.1.1 is vulnerable to SQL Injection due to improper sanitation of user-supplied input.

CVE-2011-3584 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **TYPO3 Core** - **wec_discussion** version **before 2.1.1**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Red Hat Customer Portal	Broken Link access.redhat.com text/html	MISC access.redhat.com/security/cve/cve-2011-3584

TYPO3-SA-2011-003: SQL Injection vulnerabilities in extension "WEC Discussion Forum" (wec_discussion)	Vendor Advisory typo3.org text/html	MISC typo3.org/security/advisory/typo3-sa-2011-003/
CVE-2011-3584	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2011-3584

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Guidestar	Wec Discussion Forum	All	All	All	All
Application	Guidestar	Wec Discussion Forum	All	All	All	All

cpe:2.3:a:guidestar:wec_discussion_forum:*:*:*:*:*:typo3:*:*:

cpe:2.3:a:guidestar:wec_discussion_forum:*:*:*:*:*:typo3:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→