



# CVE-2010-5102

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

## Summary

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-5102                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                        |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                  |
| <b>Published</b>       | 2012-05-21 20:55:00 UTC                                                                                                       |
| <b>Updated</b>         | 2017-08-29 01:29:00 UTC                                                                                                       |
| <b>Description</b>     | Directory traversal vulnerability in mod/tools/em/class.em_unzip.php in the unzip library in TYPO3 4.2.x before 4.2.16, 4.3.x |

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                | Product               | Version | Update | Edition | Language |
|-------------|-----------------------|-----------------------|---------|--------|---------|----------|
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.0   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.1   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.10  | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.11  | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.12  | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.13  | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.14  | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.15  | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.2   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.3   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.4   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.5   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.6   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.7   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.8   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.2.9   | All    | All     | All      |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.3.0   | All    | All     | All      |

|             |       |       |        |     |     |     |
|-------------|-------|-------|--------|-----|-----|-----|
|             |       |       |        |     |     |     |
| Application | Typo3 | Typo3 | 4.3.1  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.2  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.3  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.4  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.5  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.6  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.7  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.8  | All | All | All |
| Application | Typo3 | Typo3 | 4.4.1  | All | All | All |
| Application | Typo3 | Typo3 | 4.4.2  | All | All | All |
| Application | Typo3 | Typo3 | 4.4.3  | All | All | All |
| Application | Typo3 | Typo3 | 4.4.4  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.0  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.1  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.10 | All | All | All |
| Application | Typo3 | Typo3 | 4.2.11 | All | All | All |
| Application | Typo3 | Typo3 | 4.2.12 | All | All | All |
| Application | Typo3 | Typo3 | 4.2.13 | All | All | All |
| Application | Typo3 | Typo3 | 4.2.14 | All | All | All |
| Application | Typo3 | Typo3 | 4.2.15 | All | All | All |
| Application | Typo3 | Typo3 | 4.2.2  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.3  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.4  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.5  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.6  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.7  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.8  | All | All | All |
| Application | Typo3 | Typo3 | 4.2.9  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.0  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.1  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.2  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.3  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.4  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.5  | All | All | All |
| Application | Typo3 | Typo3 | 4.3.6  | All | All | All |

|             |                       |                       |       |     |     |     |
|-------------|-----------------------|-----------------------|-------|-----|-----|-----|
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.3.7 | All | All | All |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.3.8 | All | All | All |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.4.1 | All | All | All |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.4.2 | All | All | All |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.4.3 | All | All | All |
| Application | <a href="#">Typo3</a> | <a href="#">Typo3</a> | 4.4.4 | All | All | All |

| References                                                                                                                |        |
|---------------------------------------------------------------------------------------------------------------------------|--------|
| Reference                                                                                                                 | Source |
| 70119                                                                                                                     | OSVDB  |
| TYPO3 Core TYPO3-SA-2010-022 Multiple Remote Security Vulnerabilities                                                     | BID    |
| TYPO3 Multiple Vulnerabilities - Advisories - Community                                                                   | SECUNI |
| oss-security - CVE requests: ftpls, xdigger, lbreakout2, calibre, typo3                                                   | MLIST  |
| oss-security - CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE                                                     | MLIST  |
| Issues - TYPO3 Core - TYPO3 Forge                                                                                         | MISC   |
| TYPO3 - the Enterprise Open Source CMS: TYPO3 Security Bulletin TYPO3-SA-2010-022: Multiple vulnerabilities in TYPO3 Core | CONFIR |
| oss-security - Re: CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE                                                 | MLIST  |
| Secure Systems - Security Advisories, Audits, Testing and Research                                                        | MISC   |
| oss-security - Re: CVE-request: TYPO3 TYPO3-SA-2010-022 still without CVE                                                 | MLIST  |
| IBM X-Force Exchange                                                                                                      | XF     |
| CVE Program record                                                                                                        | CVE.OR |
| NVD vulnerability detail                                                                                                  | NVD    |

No vendor comments have been submitted for this CVE.

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