



# CVE-2014-6445

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

## Summary

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2014-6445                                                                                                                 |
| <b>State</b>           | PUBLIC                                                                                                                        |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                 |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                  |
| <b>Published</b>       | 2014-09-26 21:55:00 UTC                                                                                                       |
| <b>Updated</b>         | 2014-09-30 15:06:00 UTC                                                                                                       |
| <b>Description</b>     | Multiple cross-site scripting (XSS) vulnerabilities in includes/toAdmin.php in Contact Form 7 Integrations plugin 1.0 through |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                                     | Version | Update | Edition | Language |
|-------------|---------------------------|---------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3     | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.1   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.10  | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.2   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.3   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.4   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.5   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.6   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.7   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.8   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.9   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3     | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.1   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.10  | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.2   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.3   | All    | All     | All      |
| Application | <a href="#">Contactus</a> | <a href="#">Contact Form 7 Integrations</a> | 1.3.4   | All    | All     | All      |

|             |           |                             |       |     |     |     |
|-------------|-----------|-----------------------------|-------|-----|-----|-----|
| Application | Contactus | Contact Form 7 Integrations | 1.3.5 | All | All | All |
| Application | Contactus | Contact Form 7 Integrations | 1.3.6 | All | All | All |
| Application | Contactus | Contact Form 7 Integrations | 1.3.7 | All | All | All |
| Application | Contactus | Contact Form 7 Integrations | 1.3.8 | All | All | All |
| Application | Contactus | Contact Form 7 Integrations | 1.3.9 | All | All | All |

| References                                                  |         |                                                                   |                     |
|-------------------------------------------------------------|---------|-------------------------------------------------------------------|---------------------|
| Reference                                                   | Source  | Link                                                              | Tags                |
| CVE-2014-6445 » g0blin Research                             | MISC    | <a href="https://research.g0blin.co.uk">research.g0blin.co.uk</a> |                     |
| WordPress › Contact Form 7 Integrations « WordPress Plugins | CONFIRM | <a href="https://wordpress.org">wordpress.org</a>                 |                     |
| CVE Program record                                          | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                     | canonical           |
| NVD vulnerability detail                                    | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, analysis |

No vendor comments have been submitted for this CVE.

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