



# CVE-2013-6224

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

## Summary

|                        |                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-6224                                                                                                                      |
| <b>State</b>           | PUBLIC                                                                                                                             |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                       |
| <b>Published</b>       | 2013-12-10 16:11:00 UTC                                                                                                            |
| <b>Updated</b>         | 2017-08-29 01:33:00 UTC                                                                                                            |
| <b>Description</b>     | Multiple cross-site scripting (XSS) vulnerabilities in LiveZilla before 5.1.1.0 allow remote attackers to inject arbitrary web scr |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                   | Version | Update | Edition | Language |
|-------------|---------------------------|---------------------------|---------|--------|---------|----------|
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 3.1.8.3 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 3.2.0.2 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.0.1.0 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.0.1.1 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.0.1.2 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.1.0.3 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.1.0.4 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.2.0.4 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.2.0.5 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.0 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.1 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.2 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.3 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.4 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 3.1.8.3 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 3.2.0.2 | All    | All     | All      |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.0.1.0 | All    | All     | All      |

|             |                           |                           |         |     |     |     |
|-------------|---------------------------|---------------------------|---------|-----|-----|-----|
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.0.1.1 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.0.1.2 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.1.0.3 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.1.0.4 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.2.0.4 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 4.2.0.5 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.0 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.1 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.2 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.3 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | 5.0.1.4 | All | All | All |
| Application | <a href="#">Livezilla</a> | <a href="#">Livezilla</a> | All     | All | All | All |

| References                                                                     |          |                                              |                |  |  |  |
|--------------------------------------------------------------------------------|----------|----------------------------------------------|----------------|--|--|--|
| Reference                                                                      | Source   | Link                                         | Tags           |  |  |  |
| Full Disclosure: CVE-2013-6224: XSS in Livezilla prior version 5.1.1.0         | FULLDISC | <a href="#">seclists.org</a>                 | Exploit        |  |  |  |
| 100401                                                                         | OSVDB    | <a href="#">osvdb.org</a>                    |                |  |  |  |
| LiveZilla Changelog - LiveZilla Community Forums                               | MISC     | <a href="#">www.livezilla.net</a>            | Patch          |  |  |  |
| CVE-2013-6224: Cross Site Scripting in LiveZilla   cureblog   IT Security Blog | MISC     | <a href="#">cureblog.de</a>                  | Exploit        |  |  |  |
| 100399                                                                         | OSVDB    | <a href="#">osvdb.org</a>                    |                |  |  |  |
| 100402                                                                         | OSVDB    | <a href="#">osvdb.org</a>                    |                |  |  |  |
| IBM X-Force Exchange                                                           | XF       | <a href="#">exchange.xforce.ibmcloud.com</a> |                |  |  |  |
| LiveZilla Cross Site Scripting ≈ Packet Storm                                  | MISC     | <a href="#">packetstormsecurity.com</a>      | Exploit        |  |  |  |
| CVE Program record                                                             | CVE.ORG  | <a href="#">www.cve.org</a>                  | canonical      |  |  |  |
| NVD vulnerability detail                                                       | NVD      | <a href="#">nvd.nist.gov</a>                 | canonical, ana |  |  |  |

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)