



CVE-2018-6367

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-6367 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-01-29 05:29:00 UTC |
| Updated | 2018-02-14 14:06:00 UTC |
| Description | SQL Injection exists in Vastal I-Tech Buddy Zone Facebook Clone 2.9.9 via the /chat_im/chat_window.php request_id para |

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|----------------------------------|---------|--------|---------|----------|
| Application | Vastal | I-tech Buddy Zone Facebook Clone | 2.9.9 | All | All | All |
| Application | Vastal | I-tech Buddy Zone Facebook Clone | 2.9.9 | All | All | All |

References

| Reference | Source | Link | Tags |
|---|------------|--|--------------------------------|
| Buddy Zone 2.9.9 - SQL Injection - PHP webapps Exploit | EXPLOIT-DB | www.exploit-db.com | Exploit, Third Party Advisory, |
| Vastal I-Tech Facebook Clone 2.9.9 SQL Injection ≈ Packet Storm | MISC | packetstormsecurity.com | Exploit, Third Party Advisory, |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

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](#)