



# CVE-2008-3506

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2008-3506                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | cve@mitre.org                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2008-08-06 18:41:00 UTC                                                                                                    |
| <b>Updated</b>         | 2017-09-29 01:31:00 UTC                                                                                                    |
| <b>Description</b>     | SQL injection vulnerability in PolyPager 1.0 rc2 and earlier allows remote attackers to execute arbitrary SQL commands via |

## Risk And Classification

### Problem Types: CWE-89

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                   | Version | Update | Edition | Language |
|-------------|---------------------------|---------------------------|---------|--------|---------|----------|
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.4   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.51  | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.6   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.7   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.8   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.9   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 1.0     | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 1.0     | rc1    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.4   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.51  | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.6   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.7   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.8   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 0.9.9   | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 1.0     | All    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | 1.0     | rc1    | All     | All      |
| Application | <a href="#">Polypager</a> | <a href="#">Polypager</a> | All     | rc2    | All     | All      |

| References                                                                     |            |                                                                                 |           |
|--------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------|-----------|
| Reference                                                                      | Source     | Link                                                                            | Tags      |
| SecurityReason - PolyPager <= 1.0rc2 (SQL/XSS) Multiple Remote Vulnerabilities | SREASON    | <a href="https://securityreason.com">securityreason.com</a>                     |           |
| polypager 1.0rc2 - SQL Injection / Cross-Site Scripting - PHP webapps Exploit  | EXPLOIT-DB | <a href="https://www.exploit-db.com">www.exploit-db.com</a>                     |           |
| IBM X-Force Exchange                                                           | XF         | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |           |
| PolyPager 'nr' Parameter SQL Injection Vulnerability                           | BID        | <a href="https://www.securityfocus.com">www.securityfocus.com</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 |

No vendor comments have been submitted for this CVE.

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