



# CVE-2006-0682

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

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2006-0682                                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2006-02-15 00:02:00 UTC                                                                                                        |
| <b>Updated</b>         | 2017-07-20 01:29:00 UTC                                                                                                        |
| <b>Description</b>     | Multiple cross-site scripting (XSS) vulnerabilities in bbcodes system in e107 before 0.7.2 allow remote attackers to inject ar |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version    | Update | Edition | Language |
|-------------|--------|---------|------------|--------|---------|----------|
| Application | E107   | E107    | 0.547_beta | All    | All     | All      |
| Application | E107   | E107    | 0.548_beta | All    | All     | All      |
| Application | E107   | E107    | 0.549_beta | All    | All     | All      |
| Application | E107   | E107    | 0.551_beta | All    | All     | All      |
| Application | E107   | E107    | 0.552_beta | All    | All     | All      |
| Application | E107   | E107    | 0.553_beta | All    | All     | All      |
| Application | E107   | E107    | 0.554_beta | All    | All     | All      |
| Application | E107   | E107    | 0.555_beta | All    | All     | All      |
| Application | E107   | E107    | 0.600      | All    | All     | All      |
| Application | E107   | E107    | 0.601      | All    | All     | All      |
| Application | E107   | E107    | 0.602      | All    | All     | All      |
| Application | E107   | E107    | 0.603      | All    | All     | All      |
| Application | E107   | E107    | 0.604      | All    | All     | All      |
| Application | E107   | E107    | 0.605      | All    | All     | All      |
| Application | E107   | E107    | 0.606      | All    | All     | All      |
| Application | E107   | E107    | 0.607      | All    | All     | All      |
| Application | E107   | E107    | 0.608      | All    | All     | All      |

|             |      |      |            |     |     |     |
|-------------|------|------|------------|-----|-----|-----|
|             |      |      |            |     |     |     |
| Application | E107 | E107 | 0.609      | All | All | All |
| Application | E107 | E107 | 0.610      | All | All | All |
| Application | E107 | E107 | 0.611      | All | All | All |
| Application | E107 | E107 | 0.612      | All | All | All |
| Application | E107 | E107 | 0.613      | All | All | All |
| Application | E107 | E107 | 0.614      | All | All | All |
| Application | E107 | E107 | 0.615      | All | All | All |
| Application | E107 | E107 | 0.615a     | All | All | All |
| Application | E107 | E107 | 0.616      | All | All | All |
| Application | E107 | E107 | 0.617      | All | All | All |
| Application | E107 | E107 | 0.6171     | All | All | All |
| Application | E107 | E107 | 0.6172     | All | All | All |
| Application | E107 | E107 | 0.6173     | All | All | All |
| Application | E107 | E107 | 0.6174     | All | All | All |
| Application | E107 | E107 | 0.6175     | All | All | All |
| Application | E107 | E107 | 0.7        | All | All | All |
| Application | E107 | E107 | 0.7.1      | All | All | All |
| Application | E107 | E107 | 5.04       | All | All | All |
| Application | E107 | E107 | 5.05       | All | All | All |
| Application | E107 | E107 | 5.1        | All | All | All |
| Application | E107 | E107 | 5.2        | All | All | All |
| Application | E107 | E107 | 5.3_beta   | All | All | All |
| Application | E107 | E107 | 5.3_beta2  | All | All | All |
| Application | E107 | E107 | 5.4_beta1  | All | All | All |
| Application | E107 | E107 | 5.4_beta3  | All | All | All |
| Application | E107 | E107 | 5.4_beta4  | All | All | All |
| Application | E107 | E107 | 5.4_beta5  | All | All | All |
| Application | E107 | E107 | 5.4_beta6  | All | All | All |
| Application | E107 | E107 | 0.547_beta | All | All | All |
| Application | E107 | E107 | 0.548_beta | All | All | All |
| Application | E107 | E107 | 0.549_beta | All | All | All |
| Application | E107 | E107 | 0.551_beta | All | All | All |
| Application | E107 | E107 | 0.552_beta | All | All | All |
| Application | E107 | E107 | 0.553_beta | All | All | All |
| Application | E107 | E107 | 0.554_beta | All | All | All |

|             |      |      |            |     |     |     |
|-------------|------|------|------------|-----|-----|-----|
| Application | E107 | E107 | 0.555_beta | All | All | All |
| Application | E107 | E107 | 0.600      | All | All | All |
| Application | E107 | E107 | 0.601      | All | All | All |
| Application | E107 | E107 | 0.602      | All | All | All |
| Application | E107 | E107 | 0.603      | All | All | All |
| Application | E107 | E107 | 0.604      | All | All | All |
| Application | E107 | E107 | 0.605      | All | All | All |
| Application | E107 | E107 | 0.606      | All | All | All |
| Application | E107 | E107 | 0.607      | All | All | All |
| Application | E107 | E107 | 0.608      | All | All | All |
| Application | E107 | E107 | 0.609      | All | All | All |
| Application | E107 | E107 | 0.610      | All | All | All |
| Application | E107 | E107 | 0.611      | All | All | All |
| Application | E107 | E107 | 0.612      | All | All | All |
| Application | E107 | E107 | 0.613      | All | All | All |
| Application | E107 | E107 | 0.614      | All | All | All |
| Application | E107 | E107 | 0.615      | All | All | All |
| Application | E107 | E107 | 0.615a     | All | All | All |
| Application | E107 | E107 | 0.616      | All | All | All |
| Application | E107 | E107 | 0.617      | All | All | All |
| Application | E107 | E107 | 0.6171     | All | All | All |
| Application | E107 | E107 | 0.6172     | All | All | All |
| Application | E107 | E107 | 0.6173     | All | All | All |
| Application | E107 | E107 | 0.6174     | All | All | All |
| Application | E107 | E107 | 0.6175     | All | All | All |
| Application | E107 | E107 | 0.7        | All | All | All |
| Application | E107 | E107 | 0.7.1      | All | All | All |
| Application | E107 | E107 | 5.04       | All | All | All |
| Application | E107 | E107 | 5.05       | All | All | All |
| Application | E107 | E107 | 5.1        | All | All | All |
| Application | E107 | E107 | 5.2        | All | All | All |
| Application | E107 | E107 | 5.3_beta   | All | All | All |
| Application | E107 | E107 | 5.3_beta2  | All | All | All |
| Application | E107 | E107 | 5.4_beta1  | All | All | All |
| Application | E107 | E107 | 5.4_beta3  | All | All | All |
| Application | E107 | E107 | 5.4_beta4  | All | All | All |

|             |                       |                       |           |     |     |     |
|-------------|-----------------------|-----------------------|-----------|-----|-----|-----|
| Application | <a href="#">E107/</a> | <a href="#">E107/</a> | 5.4_beta4 | All | All | All |
| Application | <a href="#">E107</a>  | <a href="#">E107</a>  | 5.4_beta5 | All | All | All |
| Application | <a href="#">E107</a>  | <a href="#">E107</a>  | 5.4_beta6 | All | All | All |

| References                                                                      |         |  |                                                                                |               |  |  |
|---------------------------------------------------------------------------------|---------|--|--------------------------------------------------------------------------------|---------------|--|--|
| Reference                                                                       | Source  |  | Link                                                                           | Tags          |  |  |
| E107 Website System BBCode HTML Injection Vulnerability                         | BID     |  | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |               |  |  |
| IBM X-Force Exchange                                                            | XF      |  | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |               |  |  |
| e107 Unspecified BBCode Script Insertion Vulnerabilities - Advisories - Secunia | SECUNIA |  | <a href="http://secunia.com">secunia.com</a>                                   | Patch, Vend   |  |  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                | VUPEN   |  | <a href="http://www.vupen.com">www.vupen.com</a>                               |               |  |  |
| e107.org: Comments                                                              | CONFIRM |  | <a href="http://e107.org">e107.org</a>                                         |               |  |  |
| CVE Program record                                                              | CVE.ORG |  | <a href="http://www.cve.org">www.cve.org</a>                                   | canonical     |  |  |
| NVD vulnerability detail                                                        | NVD     |  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                 | canonical, au |  |  |

No vendor comments have been submitted for this CVE.

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