



# CVE-2009-3363

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

## Summary

|                        |                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2009-3363                                                                                                                   |
| <b>State</b>           | PUBLIC                                                                                                                          |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                    |
| <b>Published</b>       | 2009-09-24 16:30:00 UTC                                                                                                         |
| <b>Updated</b>         | 2017-08-17 01:31:00 UTC                                                                                                         |
| <b>Description</b>     | Cross-site scripting (XSS) vulnerability in the BUEditor module 5.x before 5.x-1.2 and 6.x before 6.x-1.4, a module for Drupal. |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                       | Product                  | Version     | Update | Edition | Language |
|-------------|------------------------------|--------------------------|-------------|--------|---------|----------|
| Application | <a href="#">Drupal</a>       | <a href="#">Drupal</a>   | All         | All    | All     | All      |
| Application | <a href="#">Drupal</a>       | <a href="#">Drupal</a>   | All         | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 5.x-1.0     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 5.x-1.1     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 5.x-1.x-dev | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.0     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.1     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.2     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.3     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.x-dev | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 5.x-1.0     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 5.x-1.1     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 5.x-1.x-dev | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.0     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.1     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.2     | All    | All     | All      |
| Application | <a href="#">Ufku Bayburt</a> | <a href="#">Bueditor</a> | 6.x-1.3     | All    | All     | All      |

|                                                                                                                      |              |          |             |     |         |                            |
|----------------------------------------------------------------------------------------------------------------------|--------------|----------|-------------|-----|---------|----------------------------|
| Application                                                                                                          | Ufku Bayburt | Bueditor | 6.x-1.x-dev | All | All     | All                        |
| References                                                                                                           |              |          |             |     |         |                            |
| Reference                                                                                                            |              |          |             |     | Source  | Link                       |
| Drupal BUEditor Live Preview Cross Site Scripting Vulnerability                                                      |              |          |             |     | BID     | <a href="#">www.secu</a>   |
| SA-CONTRIB-2009-055 - BUEditor - Cross Site Scripting   drupal.org                                                   |              |          |             |     | CONFIRM | <a href="#">drupal.org</a> |
| Drupal BUEditor Module Script Insertion Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com |              |          |             |     | SECUNIA | <a href="#">secunia.c</a>  |
| 57870                                                                                                                |              |          |             |     | OSVDB   | <a href="#">www.osvc</a>   |
| IBM X-Force Exchange                                                                                                 |              |          |             |     | XF      | <a href="#">exchange</a>   |
| CVE Program record                                                                                                   |              |          |             |     | CVE.ORG | <a href="#">www.cve.</a>   |
| NVD vulnerability detail                                                                                             |              |          |             |     | NVD     | <a href="#">nvd.nist.g</a> |
| No vendor comments have been submitted for this CVE.                                                                 |              |          |             |     |         |                            |
| There are currently no legacy QID mappings associated with this CVE.                                                 |              |          |             |     |         |                            |