# Alpine Linux - Bug #5238

Bug # 5237 (Closed): drupal7: Multiple Vulnerabilities (no CVE)

## [3.4] drupal7: Multiple Vulnerabilities (no CVE)

03/08/2016 11:39 AM - Alicha CH

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 03/08/2016 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 100% |
| **Category:** | Security | **Estimated time:** | 0.00 hour |
| **Target version:** | 3.4.0 | | |
| **Affected versions:** | | **Security IDs:** | |

**Description**

**CVE ID:** not yet available

### File upload access bypass and denial of service (File module - Drupal 7 and 8 - Moderately Critical)

A vulnerability exists in the File module that allows a malicious user to view, delete or substitute
a link to a file that the victim has uploaded to a form while the form has not yet been submitted and processed.
If an attacker carries out this attack continuously, all file uploads to a site could be blocked by deleting
all temporary files before they can be saved.

### Brute force amplification attacks via XML-RPC (XML-RPC server - Drupal 6 and 7 - Moderately Critical)

The XML-RPC system allows a large number of calls to the same method to be made at once, which can be
used as an enabling factor in brute force attacks (for example, attempting to determine user passwords
by submitting a large number of password variations at once). This vulnerability is mitigated by the
fact that you must have enabled a module that provides an XML-RPC method that is vulnerable to brute-forcing.
There are no such modules in Drupal 7 core, but Drupal 6 core is vulnerable via the Blog API module.
It is additionally mitigated if flood control protection is in place for the method in question.

### Open redirect via path manipulation (Base system - Drupal 6, 7 and 8 - Moderately Critical)

In Drupal 6 and 7, the current path can be populated with an external URL.
This can lead to Open Redirect vulnerabilities.

### Reflected file download vulnerability (System module - Drupal 6 and 7 - Moderately Critical)

Drupal core has a reflected file download vulnerability that could allow an attacker
to trick a user into downloading and running a file with arbitrary JSON-encoded content.

### Saving user accounts can sometimes grant the user all roles (User module - Drupal 6 and 7 - Less Critical)

Some specific contributed or custom code may call Drupal's user_save() API in a manner different than Drupal core.
Depending on the data that has been added to a form or the array prior to saving, this can lead to a user gaining all roles on a site.

### Email address can be matched to an account (User module - Drupal 7 and 8 - Less Critical)

In certain configurations where a user's email addresses could be used to log in instead of their username,
links to "have you forgotten your password" could reveal the username associated with a particular email address,
leading to an information disclosure vulnerability.

### Affected versions:

Drupal core 6.x versions prior to 6.38
**Drupal core 7.x versions prior to 7.43**
Drupal core 8.0.x versions prior to 8.0.4

## Solution:

Install the latest version:

If you use Drupal 6.x, upgrade to Drupal core 6.38
**If you use Drupal 7.x, upgrade to Drupal core 7.43**
If you use Drupal 8.0.x, upgrade to Drupal core 8.0.4

## References:

https://www.drupal.org/SA-CORE-2016-001

### Associated revisions

**Revision 88647c55 - 03/11/2016 03:19 PM - Leonardo Arena**

main/drupal7: security upgrade to 7.43. Fixes #5238

### History

**#1 - 03/11/2016 03:19 PM - Anonymous**

*- Status changed from New to Resolved*

*- % Done changed from 0 to 100*

Applied in changeset alpine:88647c550362ddfd9fef660d16d75c265df67c8d.

**#2 - 03/14/2016 11:39 AM - Alicha CH**

*- Category set to Security*

*- Status changed from Resolved to Closed*