



OrdaSoft Simple Membership and Touch Slider for Joomla: Two Flaws That Need No Login

Simple Membership for Joomla has an SQL injection in its login check, CVSS 9.3, and Touch Slider lets anyone delete or replace its slides. Versions and fixes.

Phil E. Taylor | 7 October 2026

Two CVEs published this morning by the Joomla CNA cover two more Joomla extensions from OrdaSoft. Simple Membership, which handles member registration and login, has an SQL injection in its login check that needs no account and scores CVSS 4.0 9.3 Critical. Touch Slider, a slideshow module, lets any visitor delete its slides or replace its content, scored 6.9 Medium.

If a Joomla site you manage runs either one, update it today: Simple Membership to 7.4.0 and Touch Slider to 5.4.6. This is the fourth batch of OrdaSoft security issues in under three weeks, after OS Gallery, Real Estate Manager, Vehicle Manager and Book Library, and OS CCK.

How mySites.guru flags Simple Membership and Touch Slider

mySites.guru records the exact version of every extension on every connected Joomla site twice a day. We added both records to our Joomla vulnerability database the morning they were published, so any connected site running Simple Membership below 7.4.0 or Touch Slider below 5.4.6 is now flagged on its own site card and in its audit, with the version that resolves it. If the extension is on the site, the flag is already there.

Both extensions also install a Joomla package alongside the component or module, and we flag the package too, so a site whose component or module row is missing is still caught. The flags cover every edition. Some Simple Membership Pro sites report versions in the 3.x and 4.x range, below 7.4.0, so they are flagged as well, and OrdaSoft has not said which Pro build has the fix.

Simple Membership: SQL injection in the login check, CVE-2026-102782

Simple Membership's front-end entry point, `site/simplemembership.php`, answers `task=checkLoginPass` without any authentication or access check. That much is

normal for a login check, since the visitor is not logged in yet. The handler then reads the login name from the request through Joomla's generic input filter and concatenates it straight into the SQL query, with no escaping and no parameter binding.

The filter is where the false comfort comes from. Joomla's default input filter strips HTML and script tags, so a developer testing it sees angle brackets disappear and assumes the value is clean. It leaves quotes and SQL syntax alone, and a single quote is all an attacker needs to close the login string and append their own SQL.

9.3

CVSS 4.0

CRITICAL

Joomla CNA · [CVE-2026-102782](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/S

I:N/SA:N

▼ [What does this mean?](#)

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet

AC:L Low: Nothing to work around, it just works

AT:N None: Works against any affected install

PR:N None: No account needed

UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:H High: Everything the site holds can be read

VI:H High: Data and files can be altered at will

VA:H High: The site can be taken down

What it does beyond the site

SC:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

The vector is the worst shape there is: reachable over the network, no privileges, no user interaction, and high impact on the confidentiality, integrity and availability of the data. A membership extension's database holds exactly the records an attacker wants, starting with the Joomla users table and its password hashes.

A malicious actor could extract your whole database: usernames, emails, password hashes, session IDs, shopping orders, invoices, and everything else it holds. Gulp.

The fix for this class of bug is old and simple: bind the login name as a query parameter, or at the very least pass it through `$db->quote()`. An input filter decides what a value may contain. Making it safe inside SQL is the query's job.

Touch Slider: anyone can delete or replace the slides, CVE-2026-102781

Touch Slider is a Joomla module, and it does its data management (adding, deleting and importing slides) through a single AJAX handler, `modOsTouchSliderHelper::getAjax()`, which Joomla's core `com_ajax` endpoint calls on the module's behalf. According to the record, that handler does not check who is calling: it has no user check, no permission check and no form token.

The record confirms two ways to abuse it, both anonymous:

- A plain GET request deletes any slider image by its ID. The IDs are sequential, so an attacker can walk through them and empty every slider on the site.
- A multipart upload of a zip file replaces the slider's two database tables, `#__os_touch_slider` and `#__os_touch_slider_text`, across the whole site with whatever the attacker supplies. This path does not even need a `task` parameter.

6.9

CVSS 4.0

MEDIUM

Joomla CNA · CVE-2026-102781

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet

AC:L Low: Nothing to work around, it just works

AT:N None: Works against any affected install

PR:N None: No account needed

UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:N None: Nothing can be read

VI:L Low: Some data can be altered

VA:L Low: The site slows or stutters

What it does beyond the site

SC:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

The score is Medium because the flaw cannot read data and touches only the slider's own tables. On many Joomla sites, though, the slider is the first thing a visitor sees on the home page, and an attacker who can replace its slides and text controls that space.

Which versions fix each extension

Extension	Joomla element	Affected	Fixed in
Simple Membership	<code>com_simplemembership</code>	1.0.0 to below 7.4.0	7.4.0
Touch Slider	<code>mod_os_touchslider</code>	1.0.0 to 5.4.5	5.4.6

Touch Slider's record is consistent: its title says "below 5.4.6" and its affected range stops at 5.4.5. Simple Membership's is not. The title gives the fix as "below 7.4.0", while the structured affected range runs up to and including 7.4.0, the same split that [Book Library's record](#) had last week.

Simple Membership: take the newest release

mySites.guru flags Simple Membership below 7.4.0, which is what the record title says. If OrdaSoft offers anything newer than 7.4.0, install that instead, so the question of which half of the record is right stops mattering.

OrdaSoft has not announced either fix

As far as we can find, OrdaSoft has published no advisory, no changelog entry and no security notice for either extension. The only reference in each record is the OrdaSoft home page, and neither record credits a finder. The fixed version numbers in this post come from the CVE records alone, which is now the pattern for every OrdaSoft disclosure this month.

That leaves site owners with less to go on than they need. A changelog would settle the Simple Membership range, say whether the Pro builds were patched, and say whether OrdaSoft's other slider modules share Touch Slider's AJAX handler. Until OrdaSoft says something, if you run any OrdaSoft component, check its version against the vendor's newest release whenever a new batch of records appears.

What the mySites.guru database shows

Neither extension is common, and only a small number of connected sites run either one. On the day the records were published, every install we can see is on an affected release. That is normal on the first day of a disclosure, and it is the reason we flag sites the same morning rather than waiting for owners to read a CVE feed they do not follow.

What to do today

1. Update Simple Membership to 7.4.0 or later and Touch Slider to 5.4.6 or later.
2. If you cannot update Touch Slider today, unpublish or uninstall the module.
3. If you cannot update Simple Membership today, block front-end requests containing `task=checkLoginPass` at the web server, or disable the component if

the site can manage without member logins for a day.

4. On any site that ran an affected Simple Membership version, treat the database as read: reset Super User passwords, rotate the Joomla secret, and replace stored API keys or mail credentials.
5. Check the Super User and Administrator groups for accounts your team did not create.

Find Super User accounts you did not create

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

What to check after the flag

The version flag tells you a site is exposed. It does not tell you whether anyone got there first, and an SQL injection in a login handler is the kind of thing that gets scripted and sprayed at every site that answers the right URL.

mySites.guru runs the follow-up checks as part of the subscription, unattended, on every connected site. The [rogue admin check](#) lists Super Users added outside the normal flow across your whole account in one view. The [malware and file scanners](#) look for code dropped on the server once an attacker has a password. And the [vulnerable extension list](#) explains how version flags like these work for every Joomla and WordPress extension we track.

If one of your sites already shows signs of compromise, work through [our Joomla hacked-site guide](#) or have us [fix it for you](#).

If you manage Joomla sites for clients, [mySites.guru](#) flags every connected site the day a fix like this is published, and the [free audit](#) shows what it finds on your own sites first.

Further Reading

- [CVE-2026-102782 record](#) - Simple Membership SQL injection, CWE-89.
- [CVE-2026-102781 record](#) - Touch Slider missing access control, CWE-284.
- [OWASP SQL Injection Prevention Cheat Sheet](#) - parameterised queries, the fix the Simple Membership login check lacks.
- [Three OrdaSoft Joomla extensions have unauthenticated SQL injections in their sort order](#) - Real Estate Manager, Vehicle Manager and Book Library, 28 September 2026.
- [OS CCK's SQL injection and unauthenticated upload RCE](#) - the OrdaSoft disclosure of 30 September 2026.
- [OS Gallery 6.2.7 fixes an unauthenticated SQL injection and two authenticated RCEs](#) - the first OrdaSoft disclosure of the run, 20 September 2026.

Frequently Asked Questions

Which versions of Simple Membership and Touch Slider are affected?

Simple Membership is affected from 1.0.0 and fixed in 7.4.0, according to the title of [CVE-2026-102782](#). Touch Slider is affected from 1.0.0 to 5.4.5 and fixed in 5.4.6, according to [CVE-2026-102781](#). OrdaSoft has published no changelog for either, so the fixed versions come from the CVE records alone.

Does either flaw need a login?

No. Both records score the flaws with no privileges and no user interaction required. Simple Membership's SQL injection sits in the handler that checks a login, which by its nature answers anonymous visitors. Touch Slider's handler is reached through Joomla's com_ajax endpoint and checks neither the user nor a form token.

What can an attacker do with the Touch Slider flaw?

Two things, according to the record. A single anonymous GET request deletes any slider image, and the image IDs are sequential, so they are easy to guess. An anonymous upload of a zip file replaces the slider's database tables across the whole site with content the attacker supplies. The record scores it 6.9 Medium because it cannot read data, but an attacker can wipe or rewrite what the slider shows visitors.

Are the Pro editions affected too?

The records do not separate editions, so mySites.guru flags every edition in the affected range. Some Simple Membership Pro sites report versions in the 3.x and 4.x range, which are below 7.4.0 and flagged. OrdaSoft has not said which Pro build has the fix, so a Pro site should ask OrdaSoft for its current Pro package.

Is this a Joomla vulnerability?

No. These are flaws in third-party Joomla extensions from OrdaSoft, not in Joomla itself. A Joomla site without Simple Membership or Touch Slider installed is not affected. The Joomla CNA issues CVE identifiers for third-party extensions as well as for Joomla core, which is why the records are titled 'Joomla Extension'.

How do I find every site running these extensions?

By hand, you log in to each Joomla site and read its extension list. mySites.guru records every installed extension and its version on every connected site twice a day, and flags any

site running an affected version of either extension on its own site card.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com

mySites.guru

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru