9.5.1 Release Notes

Release Version 9.x

Behavioral Improvements

- We now detect whether your Concrete site and/or its add-ons are installed via Composer. If so we will disallow direct in-app updates with a helpful explanation (thanks mlocati)
- Instead of a new `redirect` method available in the login and register controller (which forwards users on the the `rcURL` query string parameter), let's just add this behavior to the existing `forward` methods on login and register. This changes less about the core and also fixes conflicts that `redirect` had with the AbstractController::redirect method.
- Improved performance of the Document Library block, especially on sites with a large amount of file folders.
- We now no longer let users move or copy system pages like Dashboard pages.
- Fixed: layout delete confirmation says "remove" but means "orphan" (thanks janscarton)
- Anonymous surveys now check IP address as well as user cookies in order to decide whether a user has voted.
- Express Entry List and Details blocks now use the Express Entry Public

- "Browse Server" now says "Select File" in CKEditor dialogs (thanks janscarton)
- In cases of extreme failure, error handling might fall back to the debug output. This is now fixed.

Bug Fixes

- Fixed bug where Production Mode Dashboard page was not installed in the Dashboard properly.
- Fixed bug where conversations weren't rendering via JS on pages.
- Fixed bug where Forgot Password link did not work.
- Fixed Page Attribute Display block not working properly.
- Fixed bug where Twig-based custom block templates weren't selectable in the UI and didn't apply properly.
- Fixed bug where themes that used the deprecated `$this` variable from within block templates would throw "Cannot access protected property" errors. (Note: if your theme or block suffers from this, you should switch to using `$b` or `$view` objects, which are auto-injected into template files.
- Fixed bug where Express form attributes not included in mail notifications.
- Fixed bug where when users copied external links, they were incorrectly created as aliases. Then, when deleted the original external link would also be deleted. Now, copying external links will create full duplicates of the external link in the sitemap.

with SMTP and to use encryption under certain circumstances. Adds options to SMTP encryption for more explicit configuration of TLS, STARTTLS, and other modes.
- Fixed some errors that occurred when attempting to upgrade from 5.7 all the way to 9.5.1.

Developer Updates

- Added new concrete/src/Url/Validation utilities for validating public URLs and building Guzzle requests to them in a secure way.
- Express Details block now assumes details loaded from an Express Entry List block use the public identifier string rather than the legacy sequential integer identifier. This should not affect you unless you have forked these blocks or have heavily customized your Express setup.

Backward Compatibility Notes

- Additional backward compatibility note: Concrete CMS 9.5.0's switch to Symfony Mailer may cause problems on systems that disable `proc_open`, since it uses this to send mail using the local sendmail binary instead of the local `mail()` function. If this is a problem, consider configuring mail to use an external SMTP server.

`Concrete\Core\Summary\Category\Driver\DriverInterface`) and you don't extend AbstractDriver, you will see an error message when attempting to render custom summary templates for this driver. You should also implement your own `canViewRenderedSummaryTemplates` permission call in your driver. (This is not common.)

Security Fixes

- Updated certain JS dependencies to new versions to resolve security issues in those upstream libraries.
- Fixed CVE-2026-8134. Prior to the fix, Concrete CMS failed to sanitize path traversal sequences in the `ptComposerFormLayoutSetControlCustomTemplate` field when saving page type composer form layouts. An authenticated rogue administrator with composer form editing rights could exploit this to include arbitrary readable files on the server. Combined with the file uploader's extension-only validation (which permits PHP code in files saved with image extensions like .png), this could result in authenticated remote code execution. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 9.4 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI :H. Thanks Yonatan Drori (Tenzai) for reporting H1 3705064.

Code Execution due to insecure deserialization in the `ExpressEntryList` block controller. A rogue administrator with privileges to add blocks to an area could bypass the intended protection mechanism (`_fromCIF === true`) by leveraging the REST API functionality, which parses requests using `json_decode()` evaluating the string `"true"` as a strict PHP Boolean(true). This bypass allowed injection of a malicious serialized payload into the block's `filterFields` database column, subsequently executed when the block's data was viewed or edited by an administrator, leading to complete server takeover. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 8.9 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI :H. Thanks Nguyễn Văn Thiện for reporting H1 3643372.

- Fixed CVE-2026-8140. Prior to the fix, Concrete CMS did not validate a CSRF token before processing requests to `/dashboard/extend/install/download/<remoteId>`. The `download()` method checked only the `canInstallPackages()` permission before fetching a remote marketplace package and writing it to the server's `DIR_PACKAGES` directory. Because the endpoint was a state-changing GET route with no token enforcement, an attacker who could cause an authenticated administrator to visit a crafted page could force an arbitrary marketplace package to be downloaded. Sites must be connected to

team gave this vulnerability a CVSS v.4.0 score of 7.5 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI:N. Thanks maru1009 for reporting H1 3588772.

- Fixed CVE-2026-8417. Prior to the fix, Concrete CMS did not validate a CSRF token before processing requests to `/dashboard/extend/update/do_update/<pkgHandle>`. The `do_update()` method checked only `canInstallPackages()` before executing `upgradeCoreData()` and `upgrade()` on the named package's controller. Because the endpoint was a state-changing GET route with no token enforcement, an attacker could force an authenticated administrator to trigger a package upgrade via a single cross-site navigation. The victim must be passing `canInstallPackages()` and the target package must already be installed to be vulnerable. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.5 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI:N. Thanks maru1009 for reporting.
- Fixed CVE-2026-8421 . Prior to the fix, Concrete CMS contained a CSRF vulnerability in the `install_package()` method of `concrete/controllers/single_page/dashboard/extend/install.php`. An attacker who could cause an authenticated administrator to visit a crafted page, and who had placed or caused a package to be present under `DIR_PACKAGES/<handle>/`, could force the installation of that package without

as the web server user and enabling remote code execution. The victim must be passing `canInstallPackages` to be vulnerable. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.5 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI: :N. Thanks maru1009 for reporting.

- Fixed CVE-2026-8426 . Prior to the fix, Concrete CMS did not validate a CSRF token before processing requests to `/dashboard/extend/update/prepare_remote_upgrade/<remoteMPID>`. An attacker who controlled the remote package returned for a known marketplace item ID could overwrite the package PHP on disk and force its `upgrade()` method to execute in a single browser navigation, resulting in remote code execution as the web server user. The victim must be passing `canInstallPackages`, the site must be connected to the Concrete marketplace, and the attacker must control the package returned for a marketplace item ID already installed on the victim site to be vulnerable. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.5 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI: :N. Thanks maru1009 for reporting.
- Fixed CVE-2026-8428 . Prior to the fix, Concrete CMS emitted a CSRF token in the `local_available_update.php` view but the corresponding `do_update()` method in `concrete/controllers/single_page/dashboard/system/update/update.php`

verification, an attacker could craft a cross-site POST that triggered a core CMS update to an attacker-specified version string. The victim must be passing `canUpgrade()` and a valid update version must be present under `DIR_CORE_UPDATES` to be vulnerable. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.5 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:A/VC:H/VI: :N. Thanks maru1009 for reporting.

- Fixed CVE-2026-8350 . Prior to the fix, Concrete CMS had missing authorization in `bulk_user_assignment.php` which could lead to privilege escalation to the Administrative Group. Any authenticated user with access to the bulk user assignment dashboard page could add any user email to any group and remove legitimate admins. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.5 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI: :N. Thanks Vincent55 for reporting H1 3594435.
- Fixed CVE-2026-8197 . Prior to the fix, Concrete CMS was vulnerable to Stored XSS via OAuth integration name. The OAuth authorize template rendered the integration name through Concrete's `t()` translation helper as a sprintf-style format, causing the integration name to land in the translated output as raw HTML. A rogue admin could potentially snoop on login submissions. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.3

Notes

9.2.5 Release Notes

9.2.6 Release Notes

9.2.7 Release Notes

9.2.8 Release Notes

9.2.9 Release Notes

9.3.0 Release Notes

9.3.1 Release Notes

9.3.2 Release Notes

9.3.3 Release Notes

Thanks Yonatan Dror (Yenzal) for reporting H1 3715243.

- Fixed CVE-2026-8203 . Prior to the fix, Concrete CMS had Stored XSS on the height parameter. The controller did not validate or sanitize `$height`, meaning any user with editor privileges could inject malicious JavaScript executing in the context of any visitor's browser, potentially leading to session hijacking, credential theft, or other malicious actions. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 7.3 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:H/VI: :N. Thanks Alfin Joseph for reporting H1 3607565.
- Fixed CVE-2026-6826 . Prior to the fix, Concrete CMS was vulnerable to unauthenticated file usage disclosure via a missing permission check in the usage controller. Any unauthenticated visitor could request `/ccm/system/dialogs/file/usage/{fID}` with any file ID and receive a list of every page referencing that file, including page IDs, handles, and full URLs, including pages otherwise restricted by permissions. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.9 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI: :N. Thanks Eldudareeno for reporting H1 3616005.
- Fixed CVE-2026-8204 . Prior to the fix, Concrete CMS had an authorization bypass in the Calendar Event Frontend Dialog which could allow cross-calendar

Notes
9.3.5 Release Notes
9.3.6 Release Notes
9.3.7 Release Notes
9.3.8 Release Notes
9.3.9 Release Notes
9.4.0 Release Notes
9.4.1 Release Notes
9.4.2 Release Notes
9.4.3 Release Notes

private calendar data. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L Thanks Winston Crooker for reporting H1 3641132.

- Fixed CVE-2026-8205 . Prior to the fix, Concrete CMS had an authorization bypass in the Calendar Block since `action_get_events` did not check `canView` on the calendar, resulting in restricted event details being disclosed. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L Thanks lalalala5678 for reporting H1 3688643.
- Fixed CVE-2026-8236 . Prior to the fix, Concrete CMS was vulnerable to IDOR combined with a missing authentication gate. The endpoint `/ccm/system/dialogs/file/usage/{fID}` accepted an integer file ID in the URL and returned internal site structure data (page IDs, versions, URL paths) to anyone who sent a GET request. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting H1 3681128.
- Fixed CVE-2026-8237 . Prior to the fix, Concrete CMS was vulnerable to IDOR via the `/ccm/frontend/conversations/message_detail` endpoint, which returned the full

Permissions and Access

Attributes

Express

Packages

REST API

Probing Further

Improvements?

Let us know by posting here.

could enumerate all conversation messages including those from restricted pages, member-only areas, and the moderation queue, with file attachments and download URLs also exposed. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Eldudareeno for reporting H1 3611476.

- Fixed CVE-2026-8238 . Prior to the fix, Concrete CMS was vulnerable to IDOR via the `/ccm/frontend/conversations/message_page` endpoint, which returned the full content of any conversation message to unauthenticated requesters. An attacker could enumerate all conversation messages including those from restricted pages, member-only areas, and the moderation queue, with file attachments and download URLs also exposed. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Tristan Madani for reporting H1 3620494
- Fixed CVE-2026-8239 . Prior to the fix, Concrete CMS was vulnerable to IDOR via the `/ccm/frontend/conversations/get_rating` endpoint, which confirmed the existence of and returned the rating score for any message by ID. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3

Thanks Tristan Madani for reporting H1 3620494.

- Fixed CVE-2026-7879 . Prior to the fix, the `submit_password()` method in `concrete/controllers/single_page/download_file.php` allowed unauthorized file access since downloading permission-restricted files bypassed the `view_file` permission check. Files without passwords could be downloaded freely, and any user who knew a file's password could download a password-protected file regardless of whether they had permission to access it. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Youssef Eid for reporting H1 3619072.
- Fixed CVE-2026-7881 . Prior to the fix, Concrete CMS was vulnerable to Insecure Direct Object Reference (IDOR) in the Express Entry Detail block via the `exEntryID` parameter, leading to unauthorized access to all Express form submissions. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3. Thanks Tristan Madani for reporting H1 3620490.
- Fixed CVE-2026-8240 . Prior to the fix, Concrete CMS was vulnerable to unauthenticated page metadata disclosure across every page with a configured summary template, revealing the existence of private, draft, and restricted pages while leaking title, path, description, and author information. The

with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting H1 3682849.

- Fixed CVE-2026-8337 . Prior to the fix, Concrete CMS was vulnerable to IDOR in surveys. On sites configured with both public and private surveys, an unauthenticated attacker could vote in a restricted survey by submitting the restricted `optionID` through the public survey's endpoint. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Zer0daySec for reporting H1 3647015.
- Fixed CVE-2026-8245 . Prior to the fix, Concrete CMS was vulnerable to Reflected XSS in Legacy Pagination via HTML attribute injection. `Concrete\Core\Legacy\Pagination` builds pagination links by raw-interpolating its `$URL` field into href="" (). Any authenticated admin or report viewer with access to `/dashboard/reports/forms/legacy` who clicked the crafted URL would fire the payload in their session. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 6.0 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Yonatan Drori (Tenzai) for reporting H1 3715249.
- Fixed CVE-2026-8327 . Prior to the fix, Concrete CMS was vulnerable to password change without

passed the entire raw POST array to `UserInfo::update()` without field whitelisting, allowing password changes without requiring the current password and while also enabling registered users to disable the per-user IP-pinning in the session validator intended to detect hijacking. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 5.3 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks 0x4c616e for reporting H1 3636712.

- Fixed CVE-2026-7882 . Prior to the fix, Concrete CMS was vulnerable to unauthorized file deletion due to an inverted CSRF token check in the `DeleteFile` controller. The code threw an error when the token was valid and proceeded with file deletion when the token was invalid or missing, effectively disabling CSRF protection for the file deletion endpoint and allowing cross-site request forgery attacks against users with permission to edit conversation messages. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Tristan Mandani for reporting H1 3626636.
- Fixed CVE-2026-7886 . Prior to the fix, Concrete CMS was vulnerable to IDOR in `AddMessage`/`UpdateMessage` via the `attachments[]` parameter, which could lead to file permission bypass. The `AddMessage` and `UpdateMessage`

files directly via `$em->find(File::class, $attachmentID)` without checking per-file permissions (`canViewFile()`), allowing any user who could post in any conversation to reference any file in the CMS file manager by its sequential ID. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Tristan Mandani for reporting H1 3626635. Note: sites with truly private files should set up a private storage location outside of the webroot so that permissions are checked on view as well.

- Fixed CVE-2026-7887 . Prior to the fix, Concrete CMS OAuth 2.0 Authorization-Code Handler bypassed account status checks. A user with `uIsActive=0` (suspended, banned, or terminated) could still authenticate via OAuth and receive valid API tokens. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N. Thanks 0x4c616e for reporting H1 3636728.
- Fixed CVE-2026-8340 . Prior to the fix, Concrete CMS was vulnerable to CSRF via `Backend\File::approveVersion`. A victim with `edit_file_contents` permission could be CSRF'd into publishing an attacker-chosen previously-uploaded version, enabling downgrade to an older file version or activation of a co-editor's unpublished

score of 2.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting H1 3682856.

- Fixed CVE-2026-8347 . Prior to the fix, Concrete CMS was vulnerable to IDOR combined with wrong authorization level in the Express association Reorder dialog, which could cause cross-entity state tampering with view-only permission on one entry. Sites using Express and relying on Express entity ordering are affected. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.3 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Winston Crooker for reporting H1 3682859.
- Thanks Yonatan Drori (Tenzai) for reporting H1 3715248 for which the following was fixed. The Concrete CMS security team gave these CSRF vulnerabilities CVSS v.4.0 scores of 2.3 with vectors CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N.
- - Fixed CVE-2026-8409. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/dialog/logs/delete`.
- - Fixed [CVE-2026-8410] (https://nvd.nist.gov/vuln/detail/CVE-2026-8410. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/dialog/logs/bulk/delete`.

Cross-Site Request Forgery (CSRF) at `concrete/controllers/dialog/page/bulk/delete`.

- Fixed CVE-2026-8412. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/dialog/page/bulk/cache`.
- Fixed CVE-2026-8413. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/dialog/page/bulk/design`.
- Fixed CVE-2026-8414. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/dialog/event/duplicate`.
- Fixed CVE-2026-8415. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/dialog/express/association/reorder`.
- Fixed CVE-2026-8416. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/backend/file addFavoriteFolder($id)`.
- Fixed CVE-2026-8427 . Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/backend/file removeFavoriteFolder($id)`.
- Fixed CVE-2026-8432. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/backend/file star()`.

Cross-Site Request Forgery (CSRF) at `concrete/controllers/backend/file rescan()`.

- Fixed CVE-2026-8434. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/backend/file rescanMultiple()`.
- Fixed CVE-2026-8435. Prior to the fix, Concrete CMS was vulnerable to Cross-Site Request Forgery (CSRF) at `concrete/controllers/backend/file approveVersion()`.
- Fixed CVE-2026-7890 Prior to the fix, the RSS Displayer block accepted a feed URL from any page editor and fetched it server-side without validation, enabling redirect-to-internal bypasses. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.1 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:L/VA:N/SC:L/SI:N/SA:N. Thanks 0x4c616e for reporting H1 3636720.
- Fixed CVE-2026-8353 by sanitizing the collection name output. Prior to the fix, Concrete CMS was vulnerable to Stored XSS via page name in the Atomik theme. A rogue editor could inject arbitrary JavaScript executing in the context of any authenticated user visiting the affected account pages, potentially leading to session hijacking, credential theft, malicious actions performed on behalf of users, and potential privilege escalation. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.1 with vector

reporting H1 3715247.

- Fixed CVE-2026-8139 . Prior to the fix, Concrete CMS was vulnerable to Stored XSS via external-link page `cvName` because `updateCollectionAliasExternal` bypassed sanitization. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.0 with vector CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Yonatan Drori (Tenzai) for reporting H1 3715245.